IES-5000/5005/6000

Integrated Ethernet Switch

Support Notes

July 2008
Edition 3

ZyXEL
Unleash Networking Power

INDEX

Application Notes

Triple play Application (with VLC Line Card)

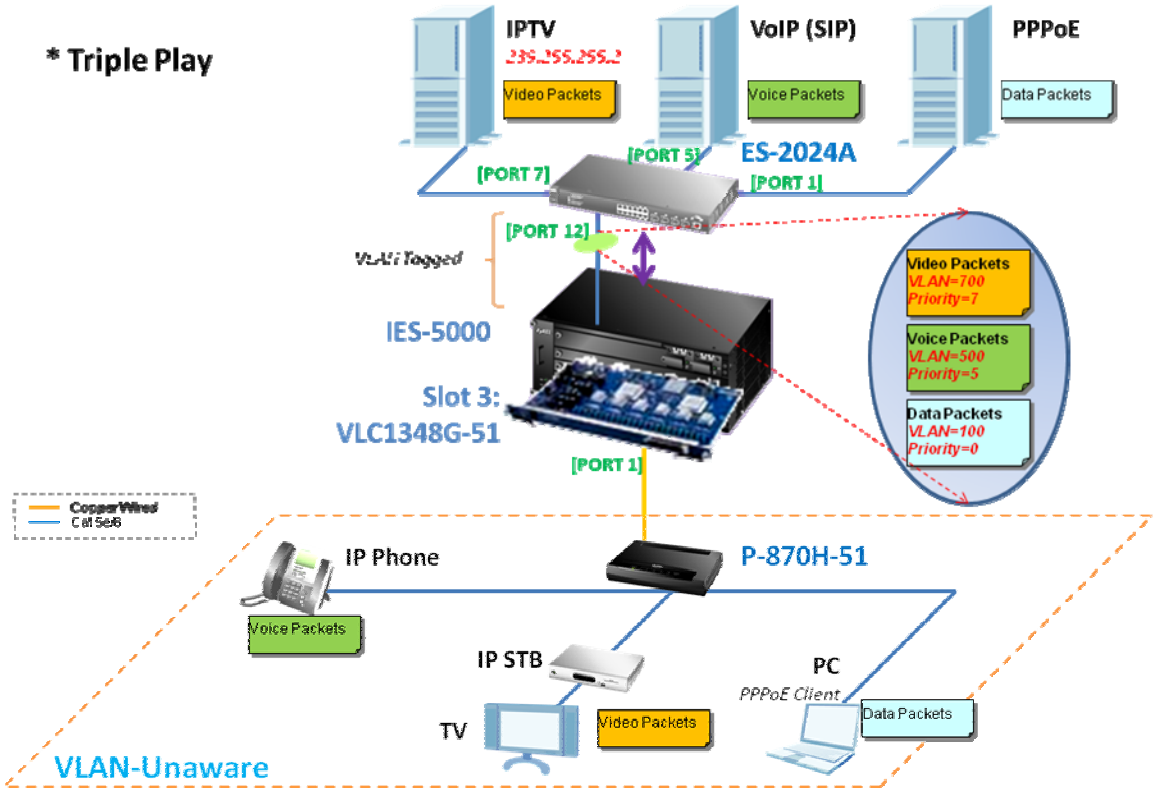
The triple play service is a marketing term for the provisioning of two broadband services, high-speed Internet access and television, and one narrowband service, telephone, over a single broadband connection. Triple Play focuses on a combined business model rather than solving technical issues or a common standard.

Triple Play

ZyXEL provides Triple Play solutions to implement triple play service in VDSL-based scenario. VDSL is a DSL technology providing faster data transmission over a single twisted pair of copper wires. These fast speeds mean that VDSL is capable of supporting new high bandwidth applications such as HDTV, as well as telephone services (Voice over IP) and general Internet access, over a single connection. VDSL is deployed over existing wiring used for POTS (Plain Old Telephone System) and lower-speed DSL connections.

The Triple Play solution is equipped with ZyXEL IES-5000 Chassis with VLC1348G-51 card, which is accompanied with P-870H-51 broadband VDSL technology CPE; the total rate can be up to 52Mbps.

Triple Play scenario topology



Hardware connections:

P-870H-51

1. **DSL:** Connect the **DSL** jack to the VLC1348G-51 card on IES-5000.
2. **Ethernet:** Connect the clients to the **Ethernet** jacks:
   (1).IP Phone to the Ethernet **1**
   (2).IP STB to the Ethernet **2**
   (3).PC to the Ethernet **3**

IES-5000M (Main Chassis)

1. Install the MSC1000G in **SLOT1**.
2. Install the VLC1348G-51 in **SLOT3**.

MSC1000G

Connect the **UP1** port of the MSC1000G to the **Port12** of the **ES-2024A**.

VLC1348G-51

1. Use a Telco-50 cable to connect to the **1-24** Telco-50 connector of the VLC1348G-51.
2. Use the **Port1** of the Telco-50 Cable to connect to the **DSL** jack of **P-870H-51**.

ES-2024A

1. Connect the **PPPoE** server (or **BRAS**) to the **Port1** of the ES-2024A.
2. Connect the **VoIP** (or **SIP server**) to the **Port5** of the ES-2024A.
3. Connect **IPTV** (or **Multicast Server**) to the **Port7** of the ES-2024A.
4. Connect **Port12** of ES-2024A to the **UP1** of the MSC1000G on IES-5000 Chassis.

Firmware versions:

ES-2024A

V3.80(TX.0)C0

IES-5000

MSC1000G: V3.90(LU.1)C0

VLC1348G-51: V3.90(BHB.0)b1

P-870H-51

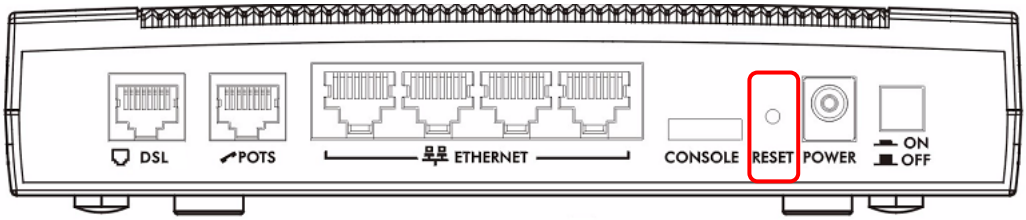
1.00(AWG.6)G0

Configure the P-870H-51:

In this scenario, we will use the CPE P-870H-51 with factory-default setting.

How to set the P-870H-51 to factory-default?

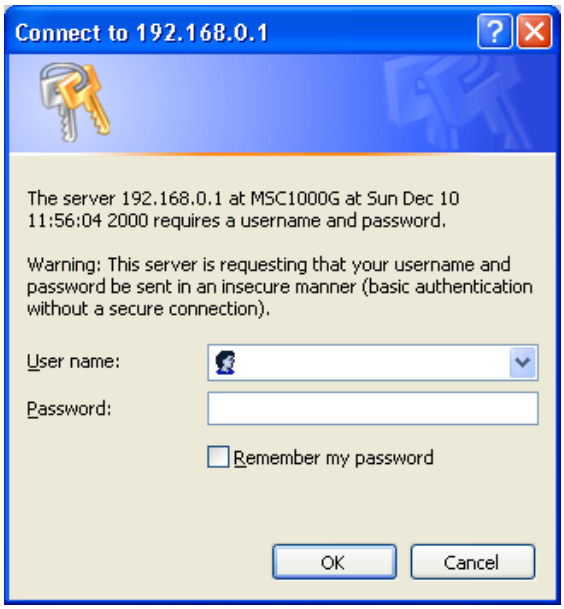
Press the **RESET** button on the back-end plane of the housing (you can see it in the following picture). Keep it pressed down for several seconds, until you see that the **POWER** LED is blinking, which means the factory default setting is being applied to the device.



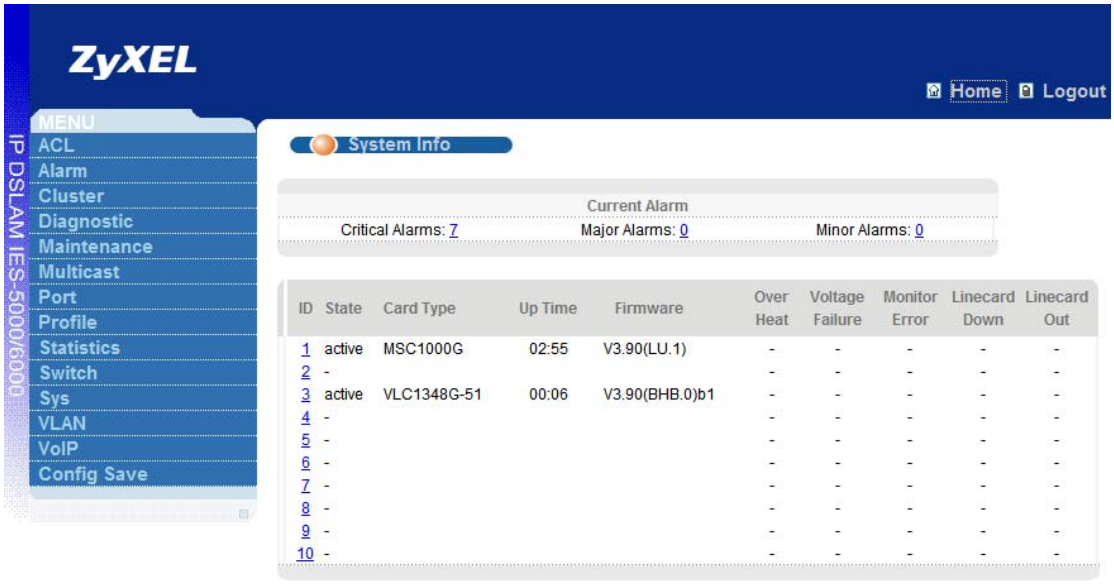
Configure the IES-5000

1. System login.

a. Connect to the IES-5000 via Internet browser. 192.168.1.1 is the default in-band management IP address and 192.168.0.1 is the default out-of-band (management port) IP address. Enter the default username (“admin”) and the password (“1234”) to access the device:



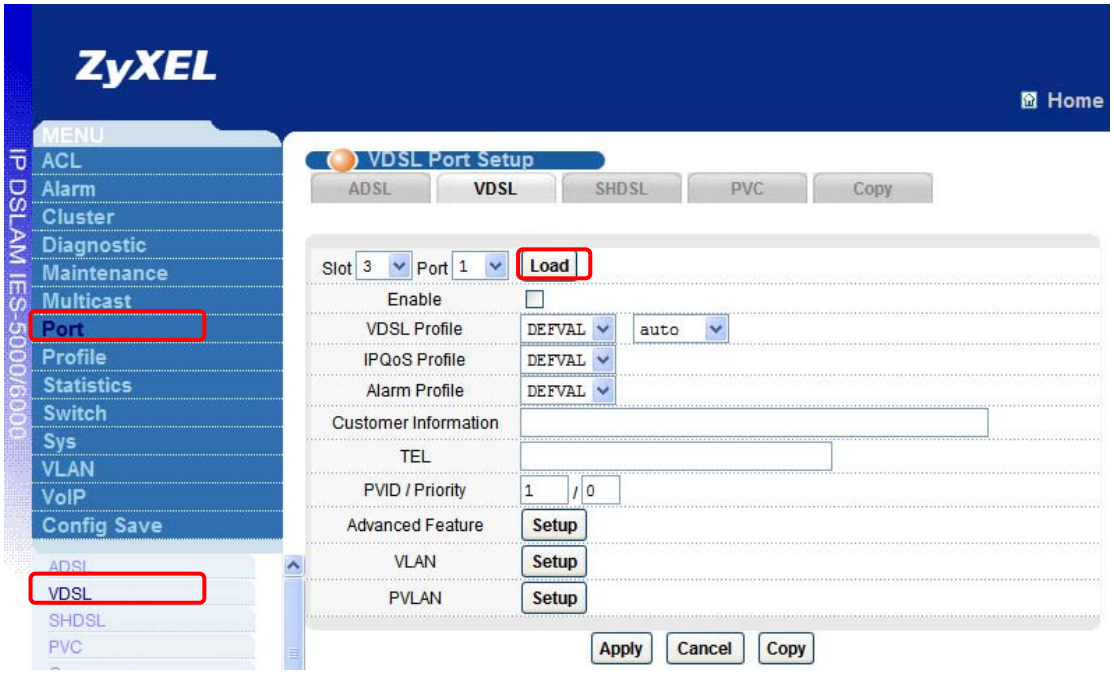
b. The main screen appears after clicking OK.



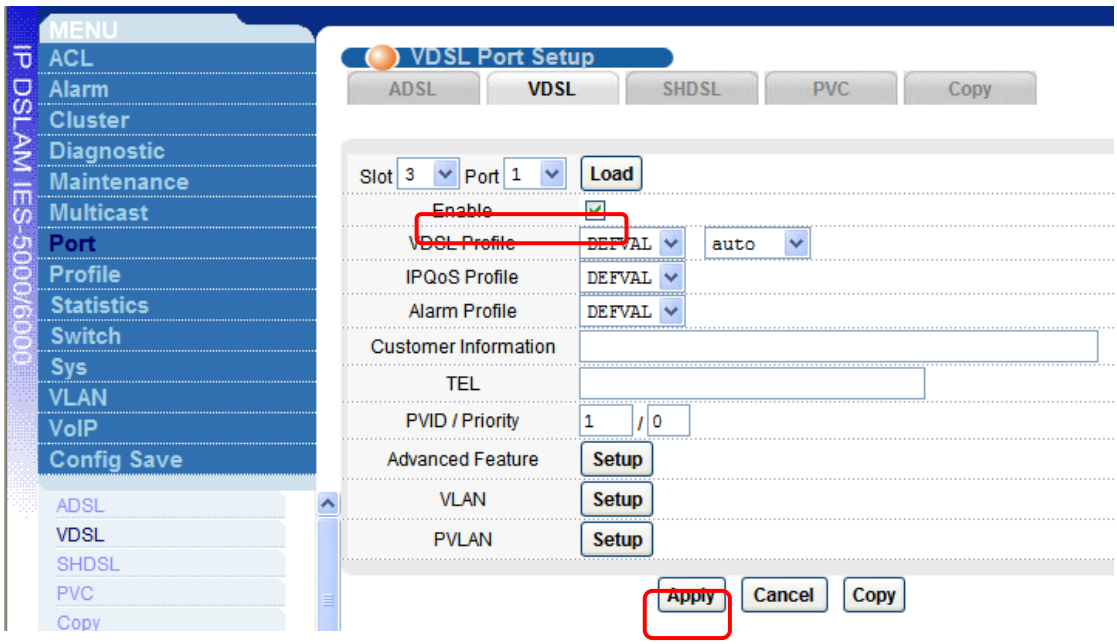
2. Configure the VLC1348G-51.

a. Click **Port > VDSL**.

b. Choose slot 3 and port 1, and click **Load** to open the page shown below:

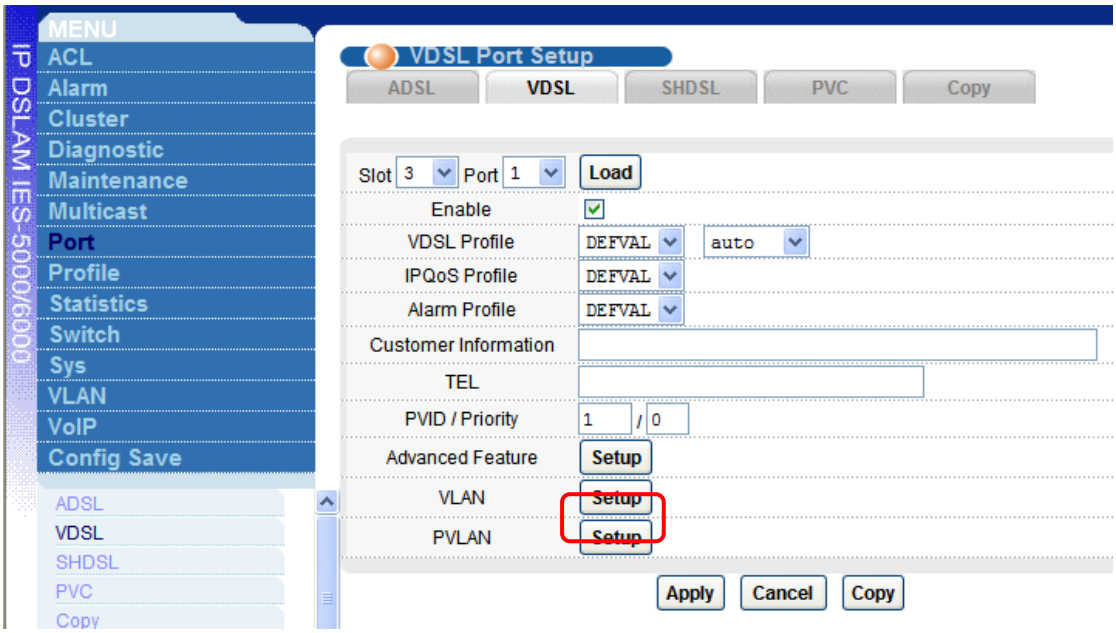


c. Select the **Enable** check-box to enable the VDSL port1, click **Apply** to save the settings**.**

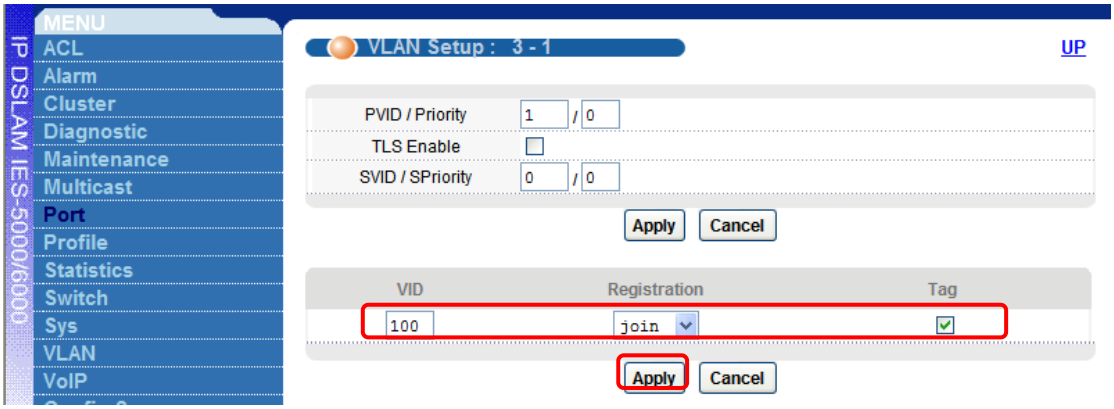


d. Click the **Setup** button in sub-step (1) of the **VLAN** to open the page relevant for sub-step (2) & (3):

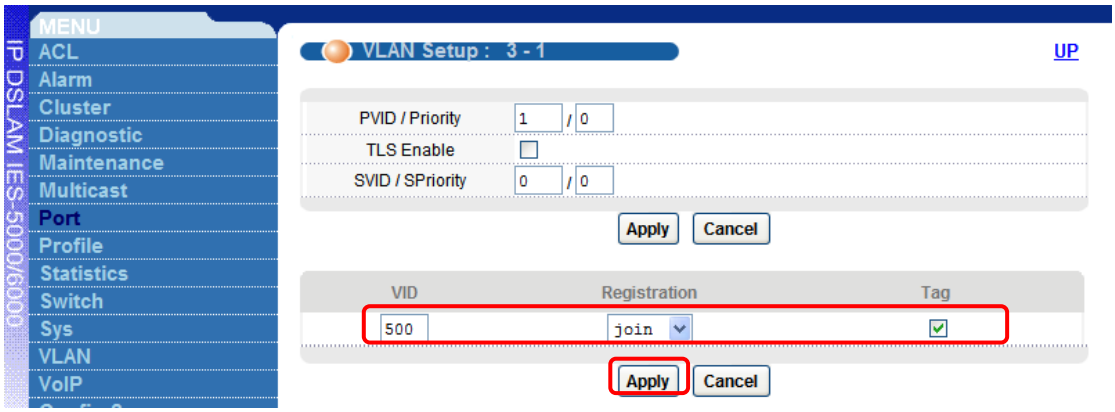
Sub-step (1): Open VLAN setup page.



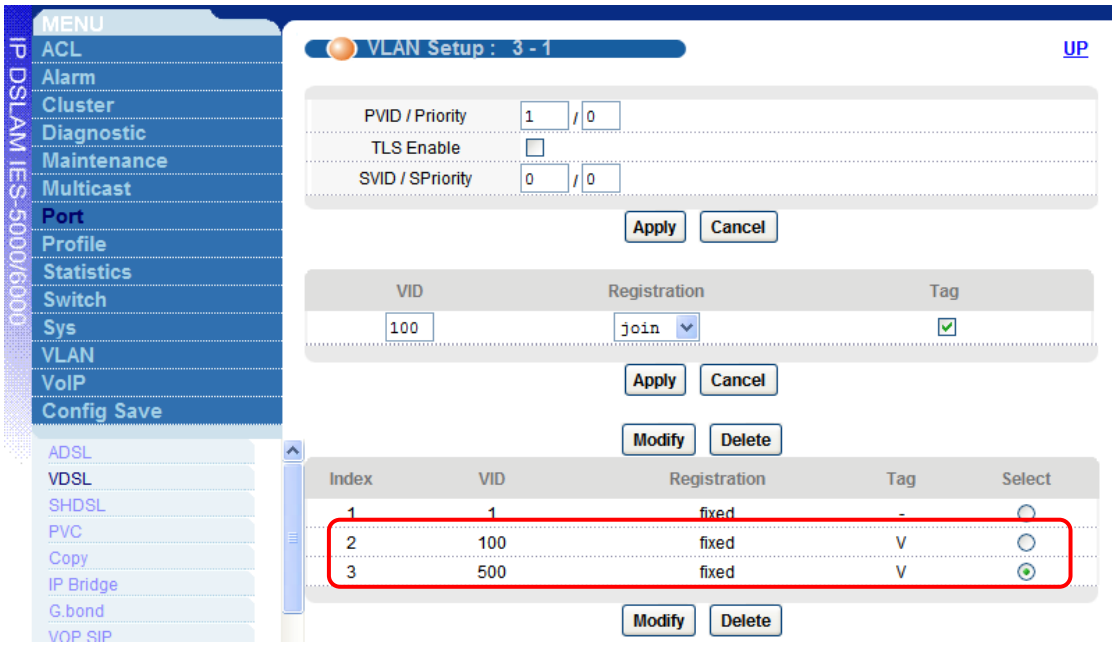
Sub-step (2): Join VLAN **100** to VDSL port 1.



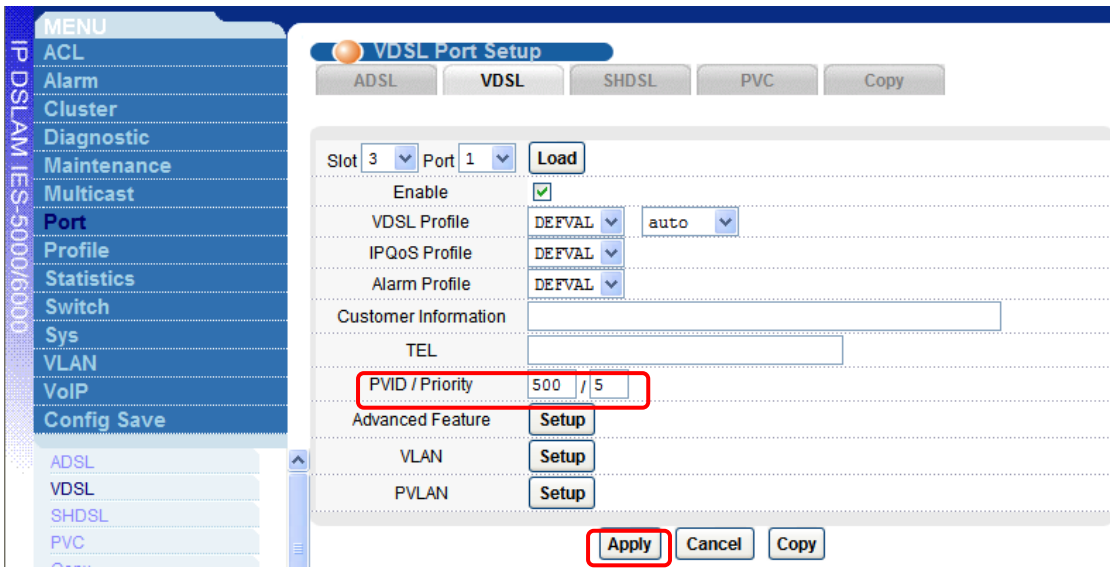
Sub-step (3): Join VLAN **500** to VDSL port 1.



Sub-step (4): Check the final VLAN setup status, you should see two entries as below.



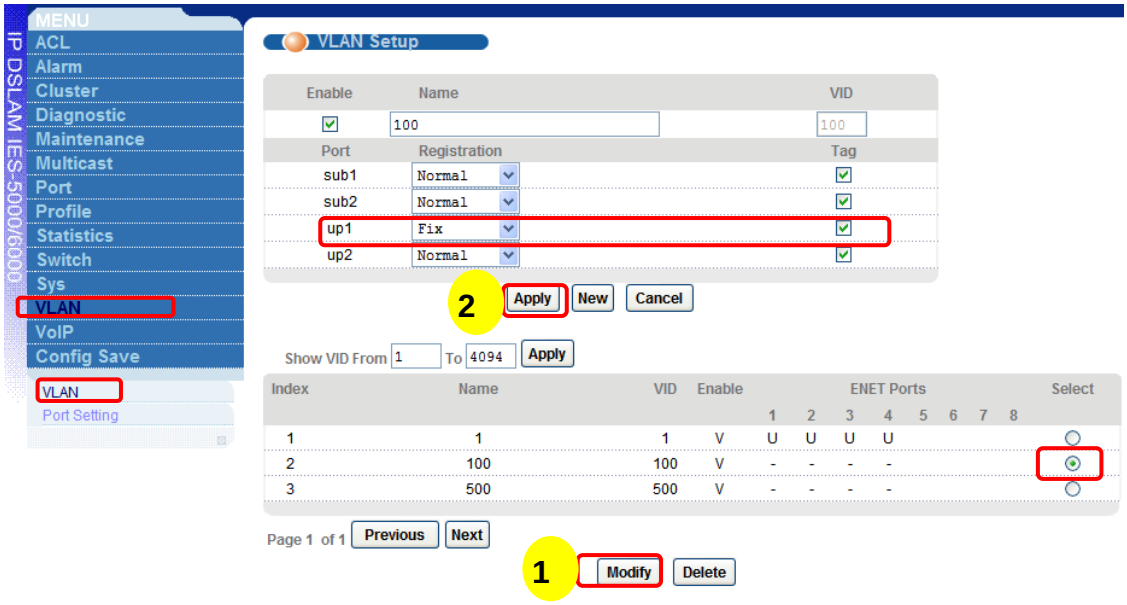
Sub-step (5): Set the default **PVID/Priority** for the VDSL **Port1**, click **Apply** to save the changes.



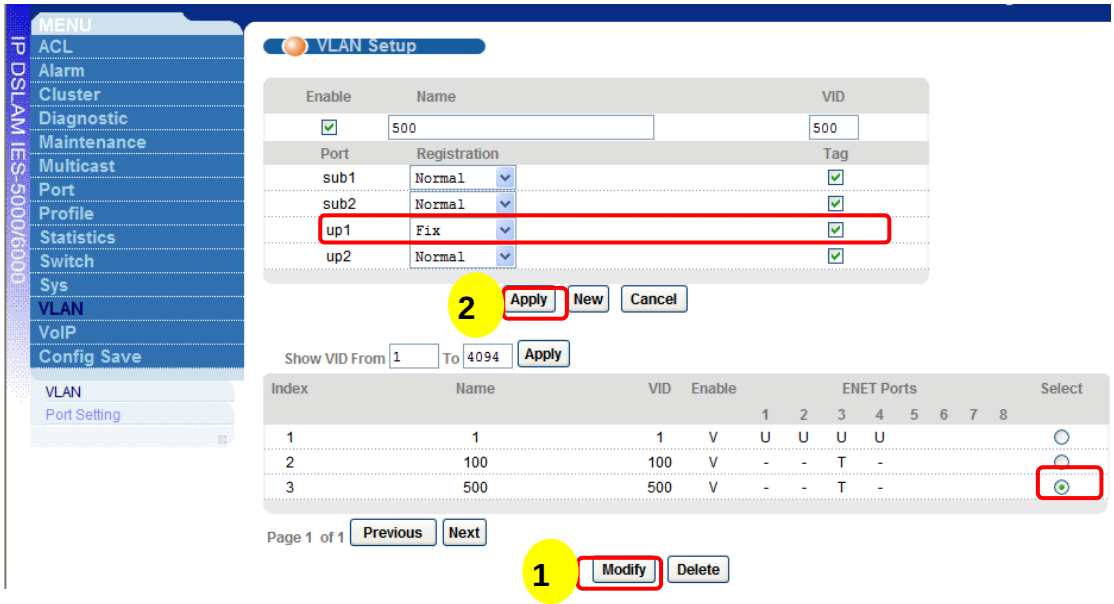
3. Configure the MSC1000G.

a. Click **VLAN** > **VLAN**

b. Select VLAN **100** and click **Modify**, then set the port **UP1** as **Fix** and **Tag**, then click **Apply** to save the changes:



c. Select VLAN **500** and click **Modify**, then set the port **UP1** as **Fix** and **Tag**, then click **Apply** to save the changes:



d. Check the final VLAN setup status of the MSC1000G

Show VID From 1 To 4094 Apply

Index	Name	VID	Enable	ENET Ports								Select
				1	2	3	4	5	6	7	8	
1	1	1	V	U	U	U	U					○
2	100	100	V	-	-	T	-					○
3	500	500	V	-	-	T	-					◉

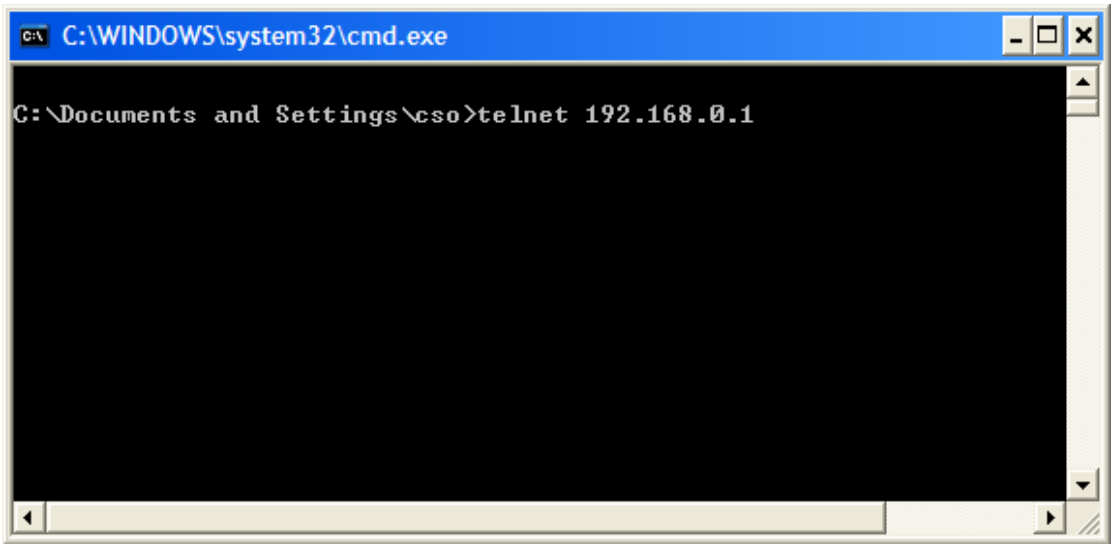
4. Use ACL rule to replace the VID / Priority for the PPPoE packets.

[Note]:

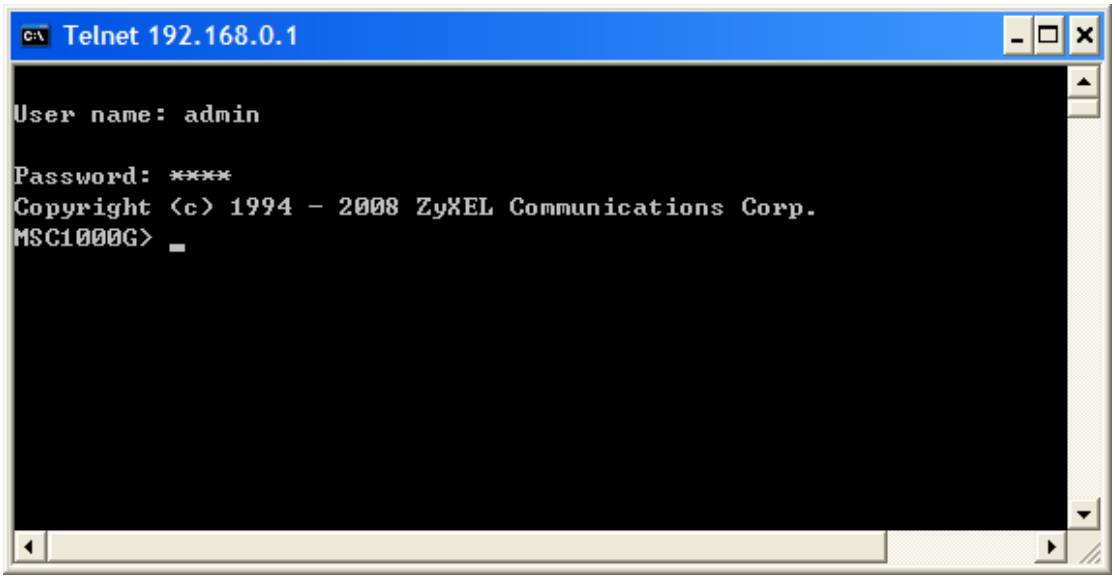
So far ACL-rule feature does not support WEB-GUI, we use the CLI method to configure it.

a. **Login**:

Connect your PC to the out-of-band **MGMT** port of MSC1000G, and call the Windows MS-DOS, then use **Telnet** method to login (use the default management IP: 192.168.0.1).



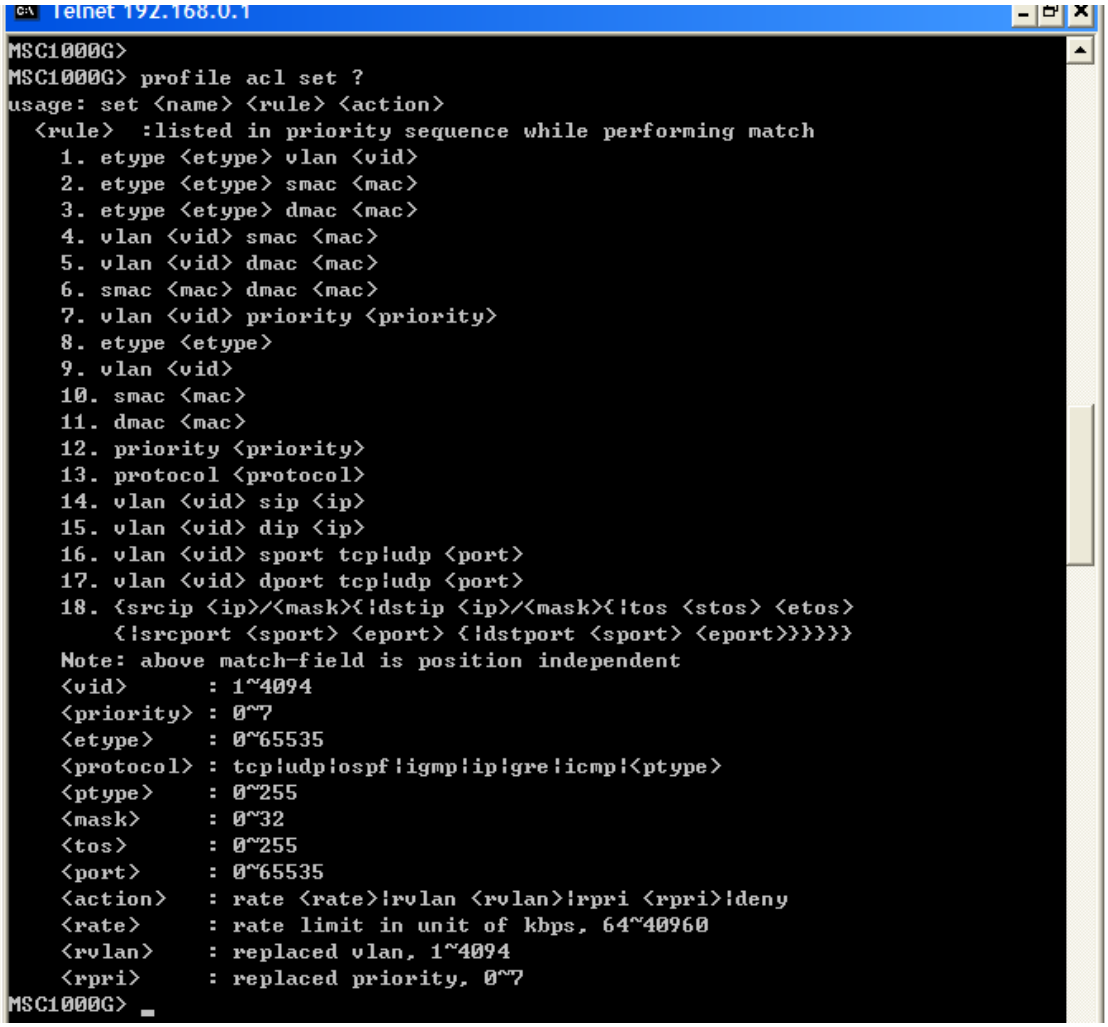
After issuing the default 'admin' / '1234' to login, you can see the page shown below:



b. **ACL-rule profile CLI syntax**:

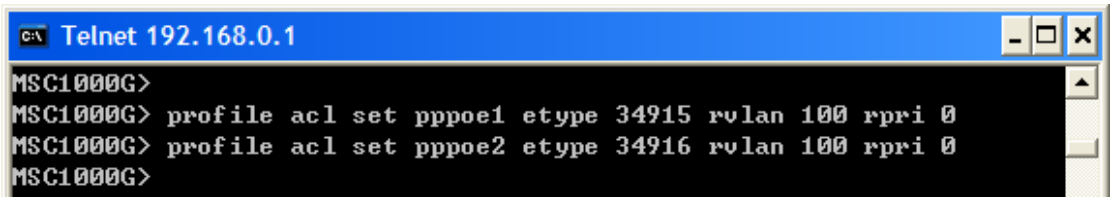
(1). <**rule**> is for picking out the traffic by specific parameters, e.g. the vid (802.1q), mac, etype (Ethernet Type), priority (802.1p) etc.

(2). <**action**> can apply actions to the traffics picked out by the <rule>, e.g. rate (limit the rate), rvlan (replace vlan), rpri (replace priority)



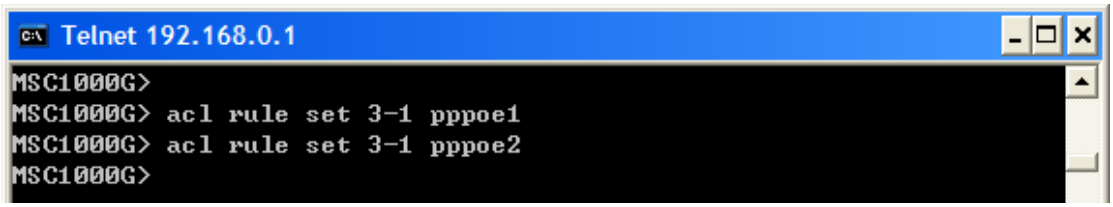
c. **Set ACL-rules to pick out PPPoE traffic and replace its VID / Priority**.

(1) Create ACL profiles



// 'pppoe1' & 'pppoe2' are the Profile names, and '34915' is the decimal value for hexadecimal value 0x8863, and '34916' is for 0x8864.//

(2) Apply the ACL profile to the VDSL port 3-1



// "3-1" represents the slot 3 and port 1, which is exactly the VDSL port we are using.//

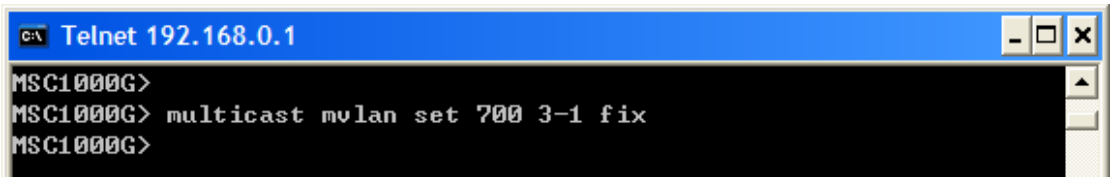
Based on the above settings, all the PPPoE traffics including the Ethernet Type: 0x8863 and 0x8864, upcoming from VDSL port 3-1 will be picked out by ACL rules 'pppoe1' and 'pppoe2', and then replaced with new VLAN ID/Priority '100/0'.

5. Use MVR to configure the IPTV setting on MSC1000G.

a. **Login**:

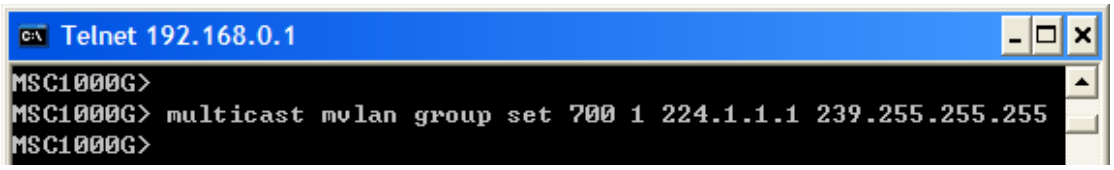
As in the **step 4**, use **Telnet** to login.

b. Set VDSL port 3-1 to join the MVR VLAN **700**.

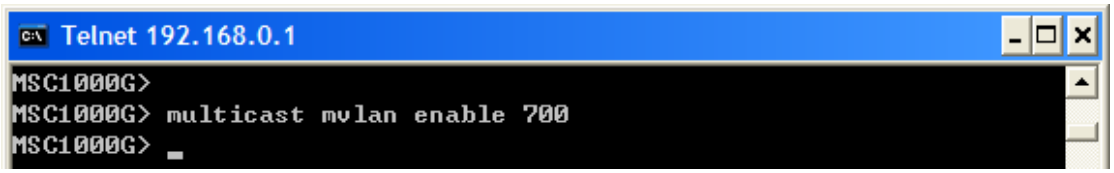


c. Set multicast **group range** for MVR VLAN 700

//Since we are using 239.255.255.2 as the multicast group IP in this case, we set the group range starting from 224.1.1.1 to 239.255.255.255//



d. **Enable** MVR VLAN 700

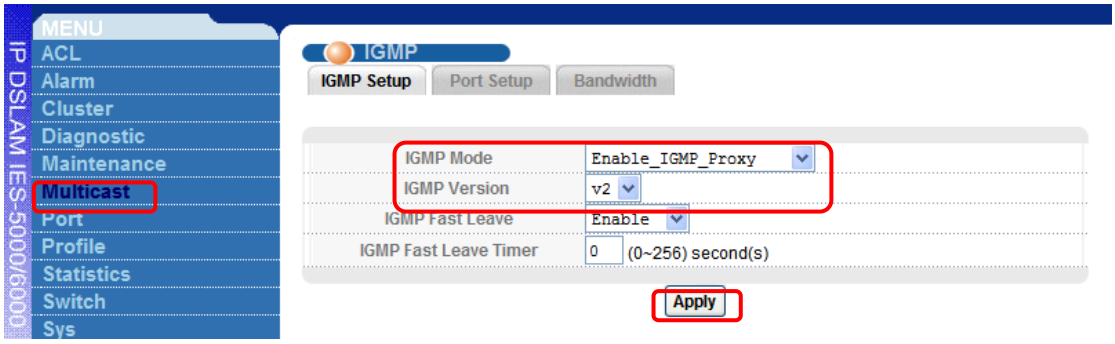


6. Configure the IGMP-Proxy and Static Query VLAN

a. **Login**:

We are using the WEB to configure again.

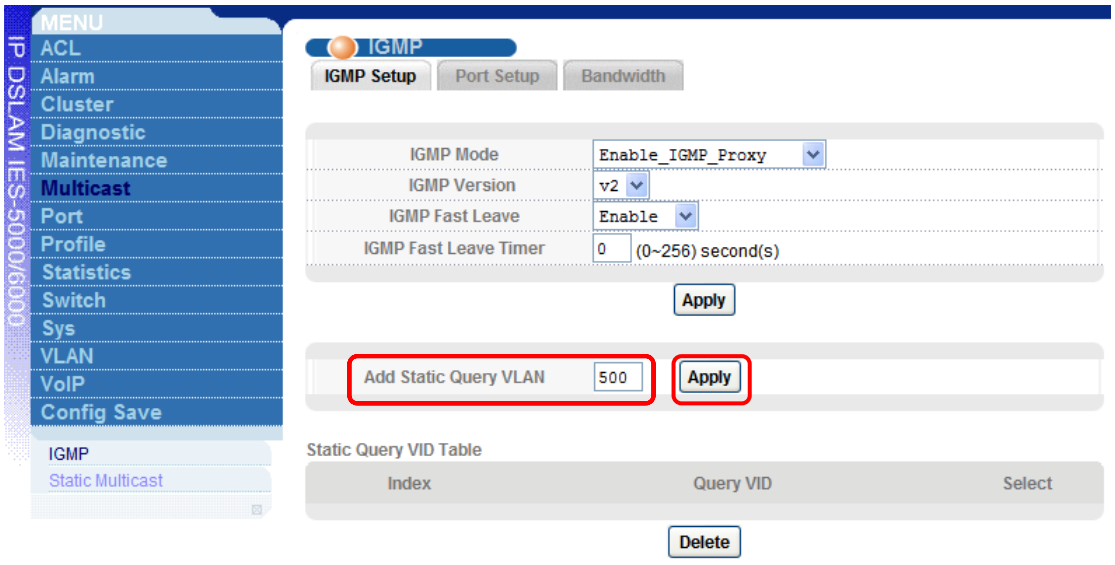
b. Click **Multicast**, then Enable **IGMP Proxy V2** mode, and click **Apply** to save the changes.



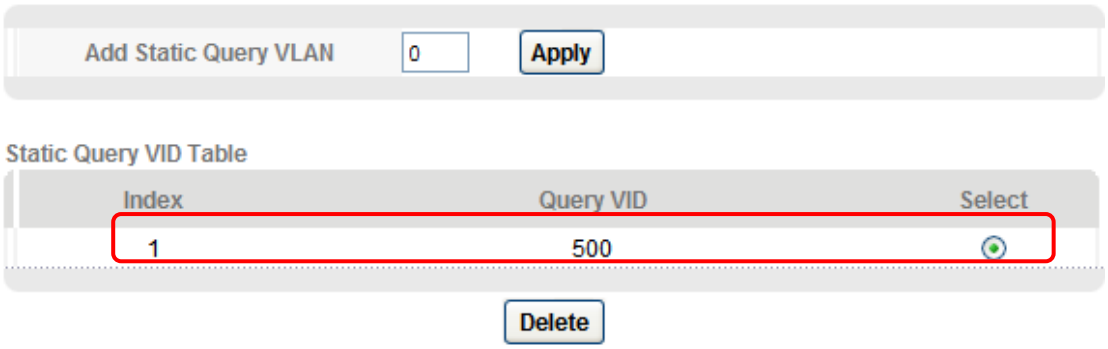
c. Add **Static Query VLAN 500**, and click **Apply** to save the changes.

[Note:] *As we don't have any IGMP-router in this scenario, Static Query VLAN should be assigned to specify the multicast service subscriber VLANs.*

// And because all the traffics sending out from the VDSL port 3-1 are untag, we can specify any VLAN joined this port, here we choose the VLAN 500. //



d. Check the Query VLAN status.



7. Save configuration for the IPDSLAM.

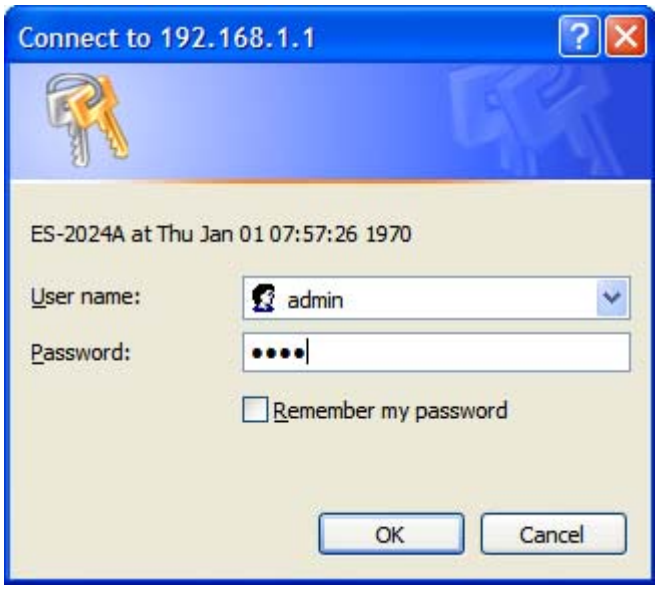
(1). Open **Config Save**, then click the **Save** button to save all your settings to NVRAM.

(2). If setting is successful, result is as below.

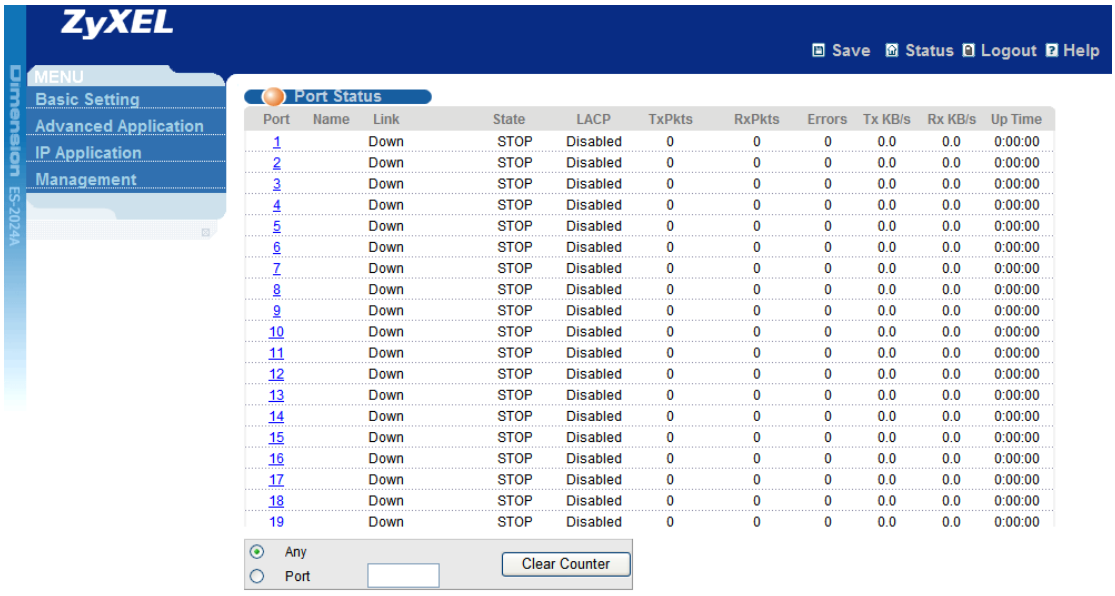
Configure the ES-2024A:

1. System login.

a. Connect to the ES-2024A via Internet browser. 192.168.1.1 is the default in-band management IP address. Enter the default username (“admin”) and the password (“1234”) to access the device:

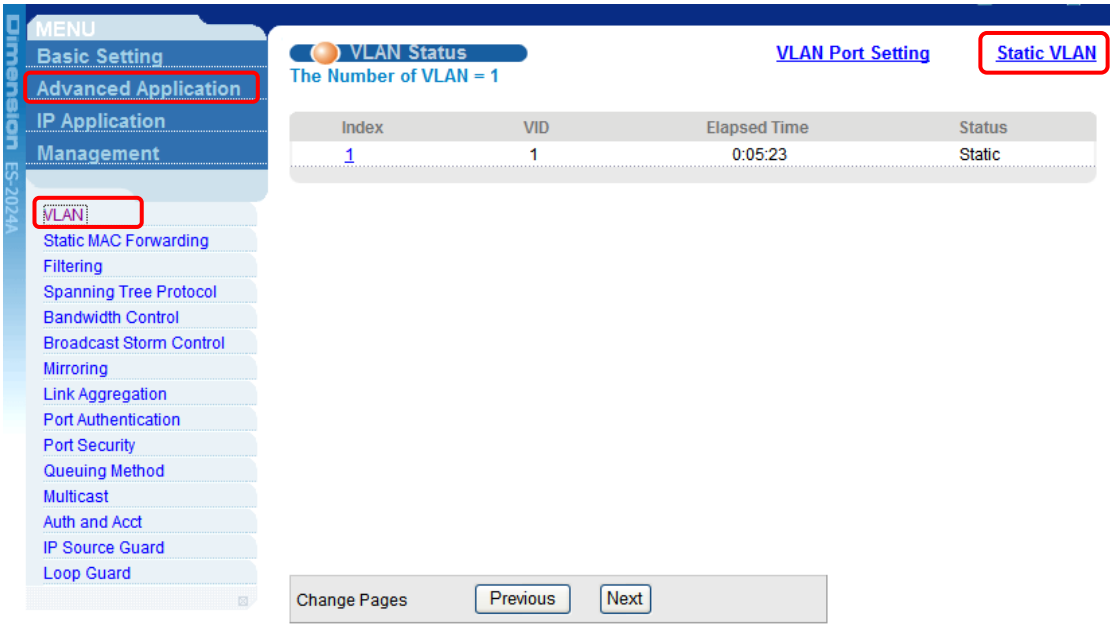


b. The main screen appears after clicking OK.



2. Configure VLANs.

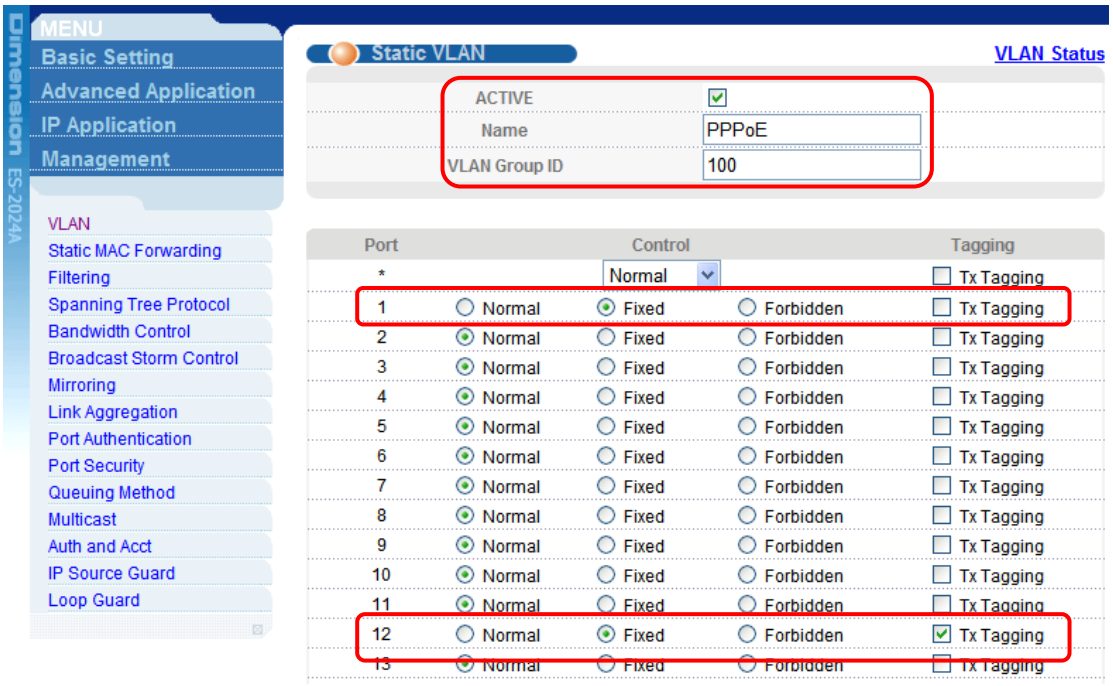
a. Click **Advanced Application** > **VLAN**, after enter the VLAN setting page, and then choose the **Static VLAN** link.



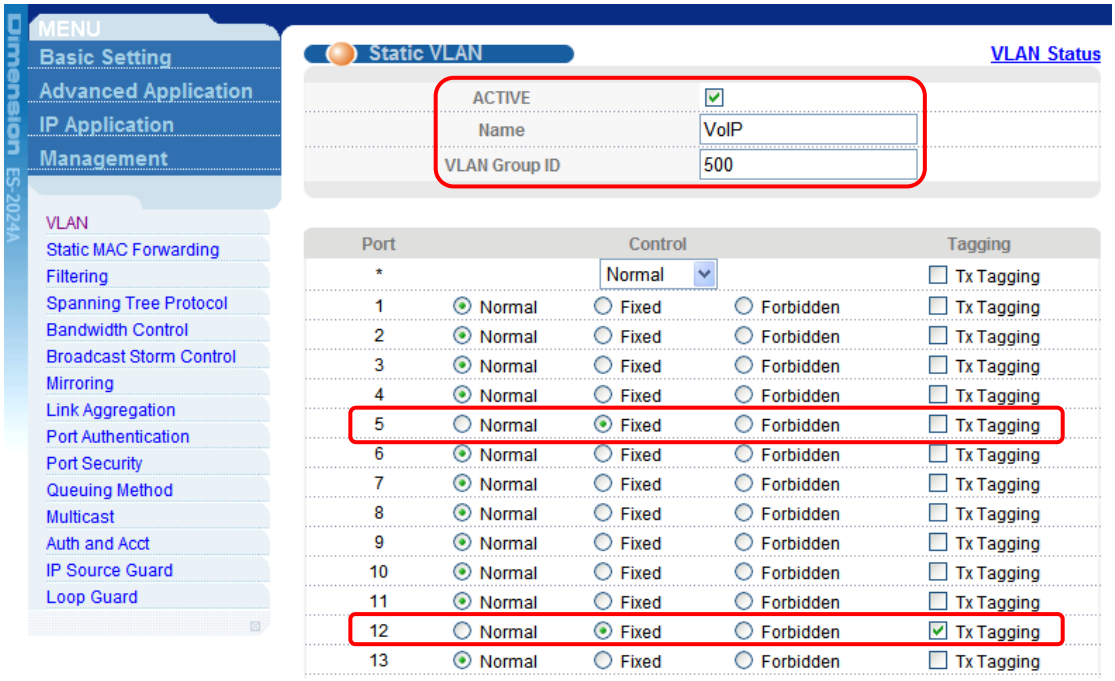
b. Create VLAN **100 / 500 / 700** for PPPoE / VoIP / IPTV respectively.

[Note:] *Don't forget to click the **Add** button at the bottom of the page.*

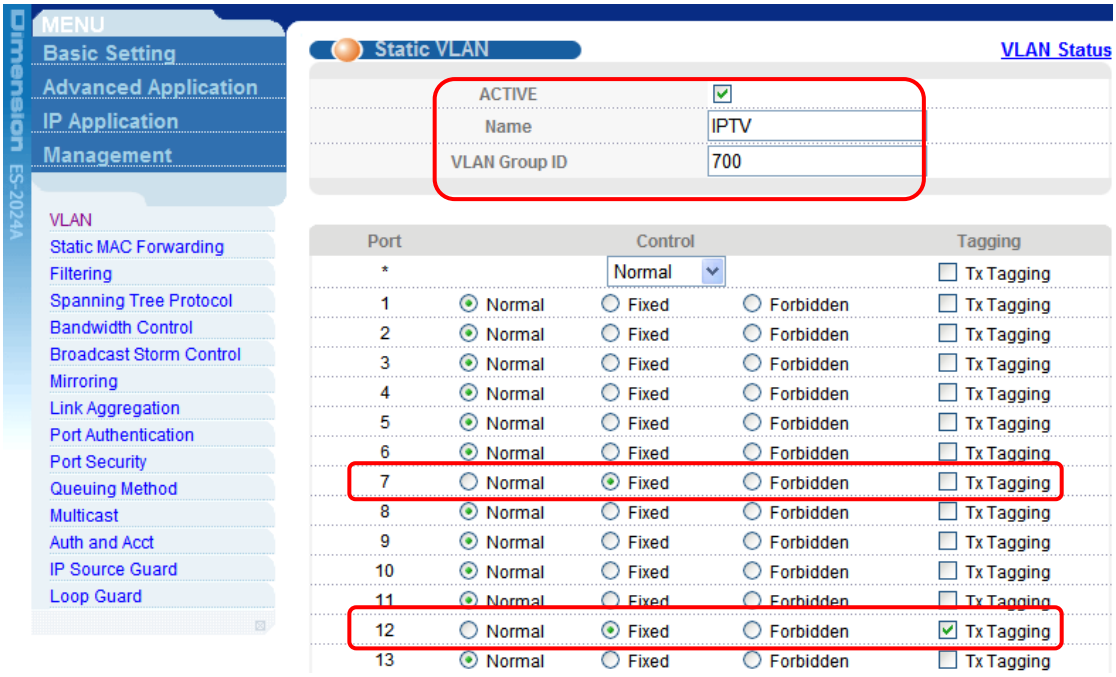
(1). VLAN 100 for PPPoE.



(2). VLAN 500 for VoIP.



(3). VLAN 700 for IPTV.

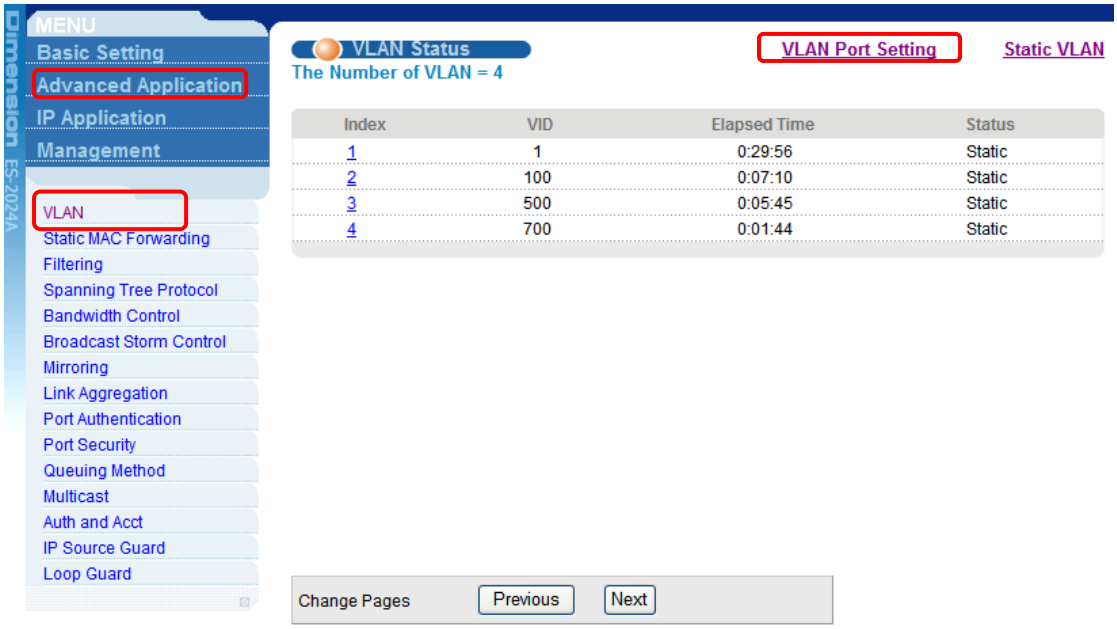


(4). Check final status of the VLAN settings.

VID	Active	Name	Delete
1	Yes	1	☐
100	Yes	PPPoE	☐
500	Yes	VoIP	☐
700	Yes	IPTV	☐

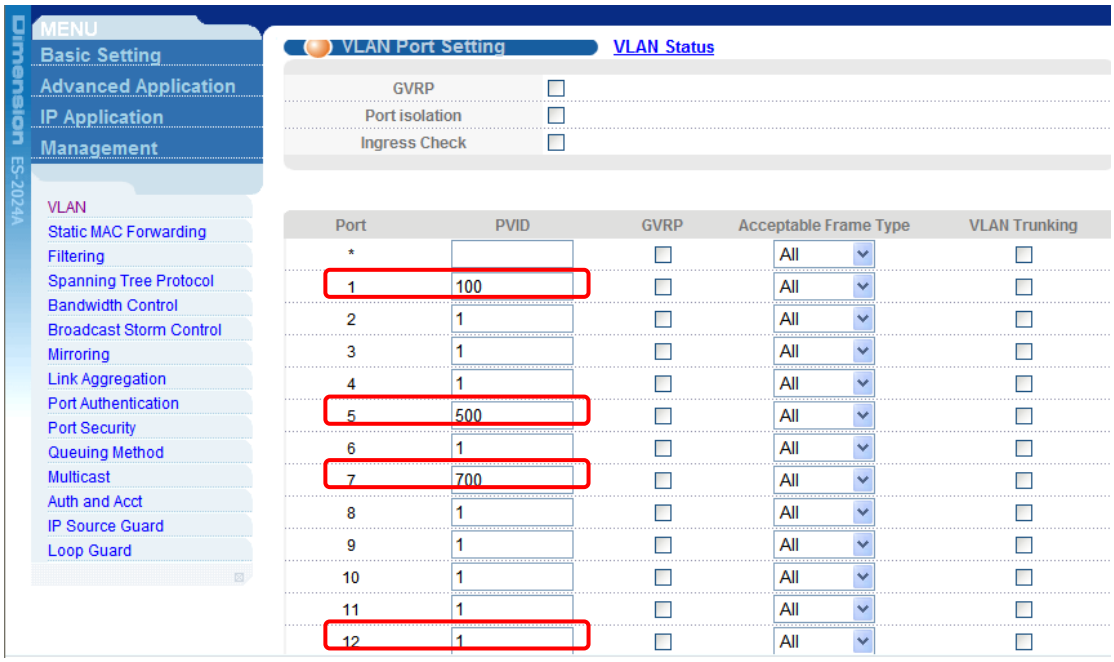
c. Set the default **PVID** for the relative ports in this scenario.

(1). Click **Advance Application** > **VLAN**, then choose the **VLAN Port Setting**



(2).Set port 1 / 5 / 7's **PVID** as 100 / 500 / 700 as below:

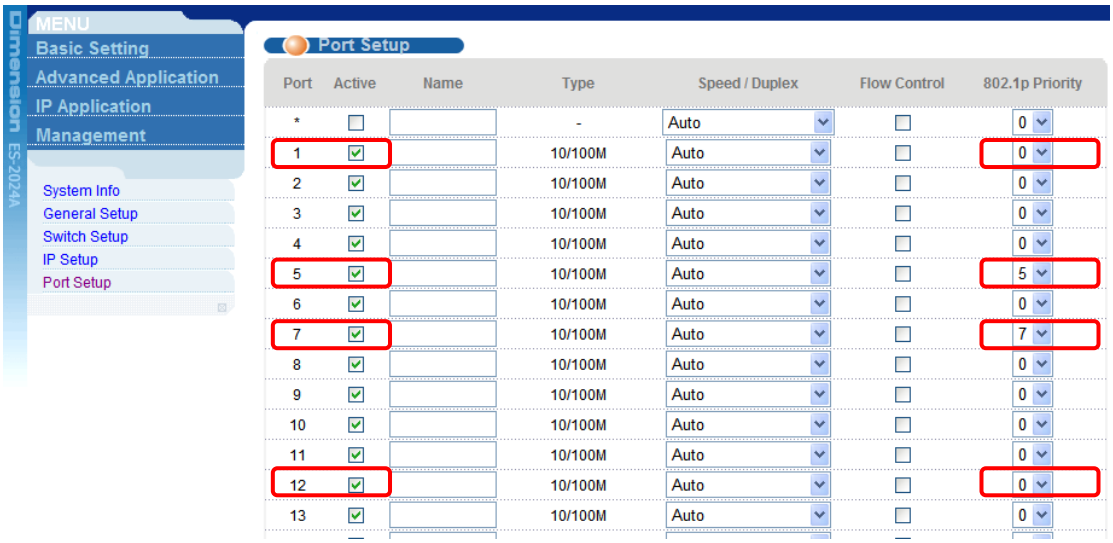
*Don't forget to click **Apply** to save the settings.*



d. Set the default **802.1p Priority** value for the respective ports in this scenario.

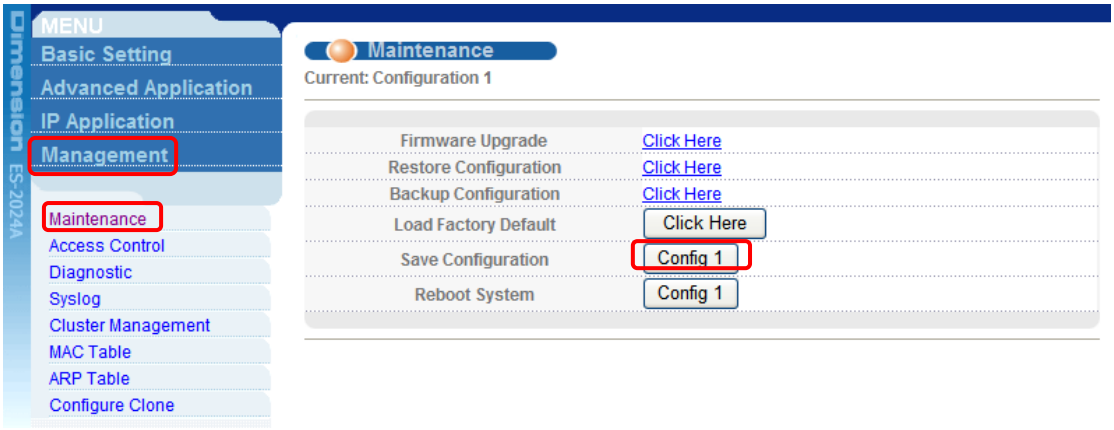
(1). Click **Basic Setting** > **Port Setup** to call the page below.

(2). Click **Apply** at bottom to save the settings.



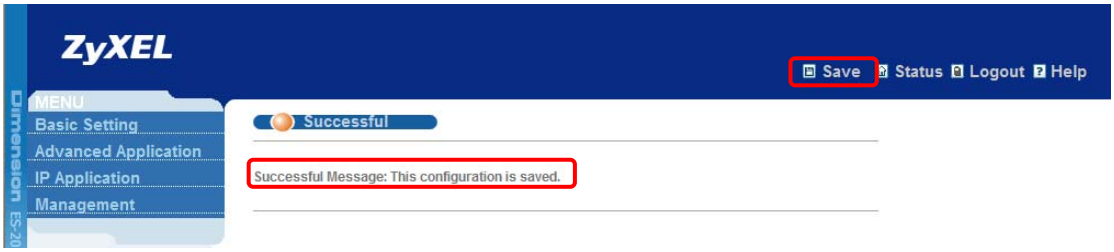
e. Save all the settings for the ES-2024A.

(1). Click **Management** > **Maintenance**, then choose the **Config 1** in Save Configuration.



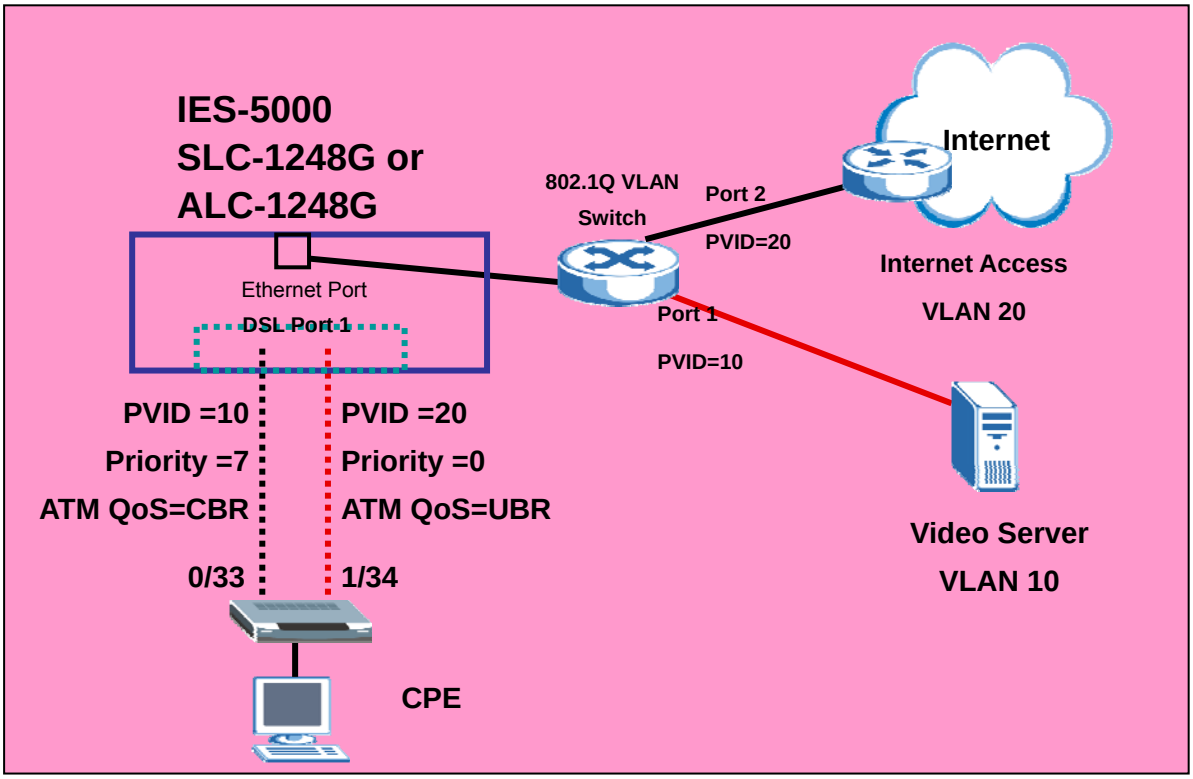
(2). Or you can choose the **Save** button on the top of the page.

If saving was successful, you would see result shown below.



Triple play Application (with ALC/SLC Line Card)

On the IES-5000, you can use different channels (also known as Permanent Virtual Circuits or PVCs) for different services. Define channels on each DSL port for different services and assign each channel a priority, VLAN and ATM Quality of Service (QoS). The ATM QoS allows you to regulate the average rate and fluctuations in data rates. This helps eliminate congestion and to allow smooth transmission of real time data (such as audio and video).
In this application, we will show you how to set up multiple PVCs using the IES-5000. The following figure shows a network example where the computers want to get different services (data service for Internet access and video service) from two networks. Since a smooth video streaming quality is desired, we want to give the video service a higher priority. To do this on the IES-5000, create a different VLAN for each service and configure the PVCs with a different VID, priority and ATM QoS. This allows the video service to have a higher priority over the data service. You can easily adapt this application for a triple-play service network.



Setting up Multiple PVCs

This section shows you how to configure settings on the devices for this application.

In this network application, we will use an IES-5000, a ZyXEL ES-2024 VLAN-aware switch and Prestige 660R-61 CPE (you may also use P791 if you have the SLC-1248G line card installed on the IES).

1. IES-5000 Settings

1.1 VLAN setup

Follow the procedure as described in the VLAN Application section to configure the VLAN settings on the IES-5000.

Create a VLAN with a VID of 10 and set Port 1 and ENET 1 to be members of this VLAN. Also enable egress tagging on ENET 1.

TGE1> vlan name 10 VLAN10
TGE1> vlan set 10 up1 fix tag
TGE1> port pvc vlan 7-1-0/33 10 join untag

Create a VLAN with a VID of 20 and set Port 1 and ENET 1 to be members of this VLAN. Also enable egress tagging on ENET 1.

TGE1> vlan name 20 VLAN20
TGE1> vlan set 20 up1 fix tag
TGE1> port pvc vlan 7-1-0/33 20 join untag

1.2 VC profile setup

For profile setup, create a Defval_CBR VC profile with the Encap, Class, PCR and CDVT settings as shown. Make sure the profile has the same LLC-based encapsulation setting as the IES-500 and the CBR class is set with a higher ATM QoS priority .

CI command

TGE1> profile atm set Def_CBR cbr 300000

1.3 Multiple PVCs setup

Since we want to give the 0/33 VPI/VCI a higher priority, change the VCI/VPI priority in the Defval_CBR profile that was just created.

CI command:

TGE1> port pvc set 7-1-0/33 Defval_CBR llc 0 7

Create another PVC with a VPI/VCI of 0/34 and apply the DEFVAL profile to this channel.

CI command:

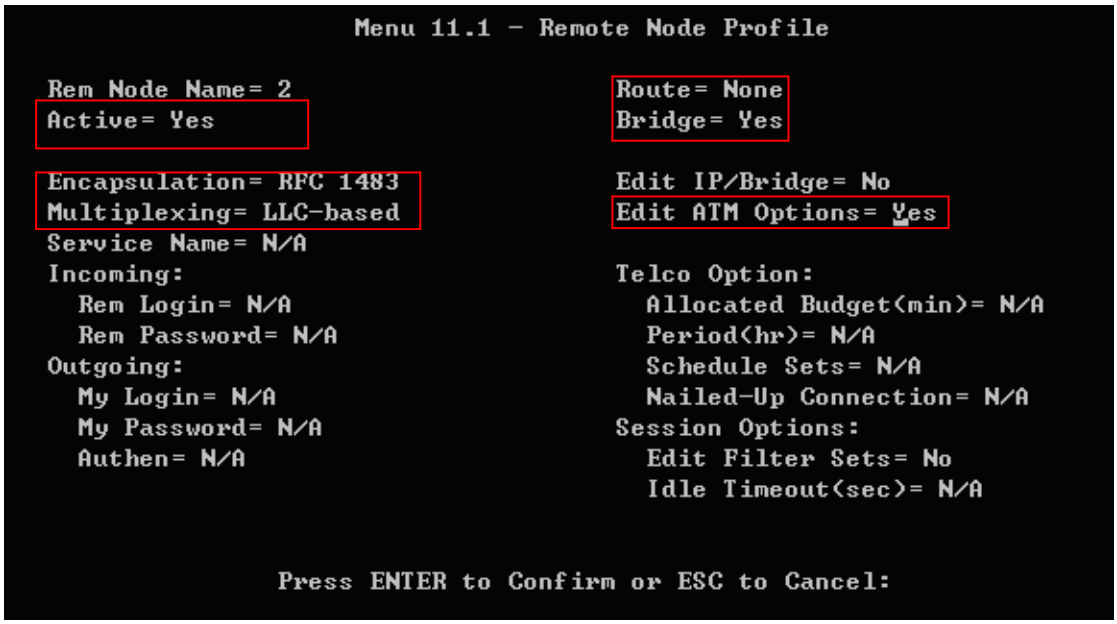
TGE1> port pvc set 7-1-0/34 Defval llc 20 0

2. Prestige 660R-61(P791) Settings

On the CPE, we need to configure two channels: 0/33 and 0/34. The previous application example already shows you how to configure a channel (0/33) on the CPE. Here, we will show you hot to configure the second channel.

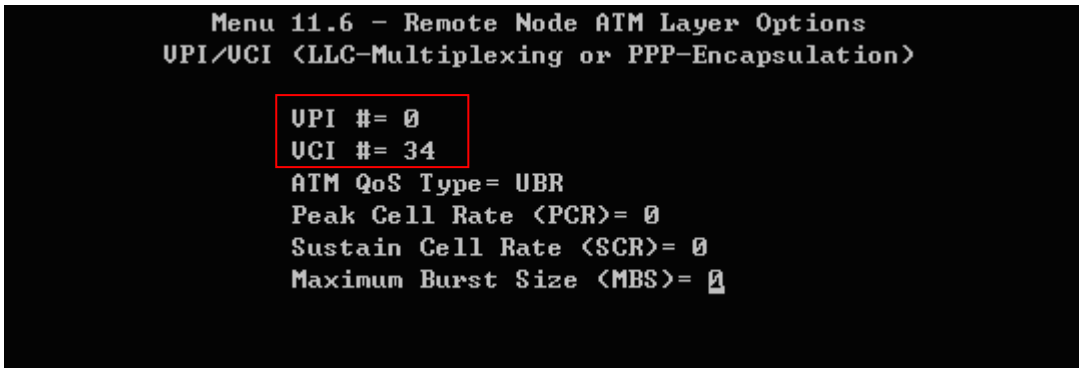
2.1 Menu11.1: Remote Node Profile

In menu 11.1, select Yes in the Active field to activate this remote node profile. Make sure the encapsulation and multiplexing settings are the same as in menu 4. Select Yes in the Edit ATM Options field and press [ENTER] to enter menu 11.6.



2.2 Menu11.6: Remote Node ATM Layer Options

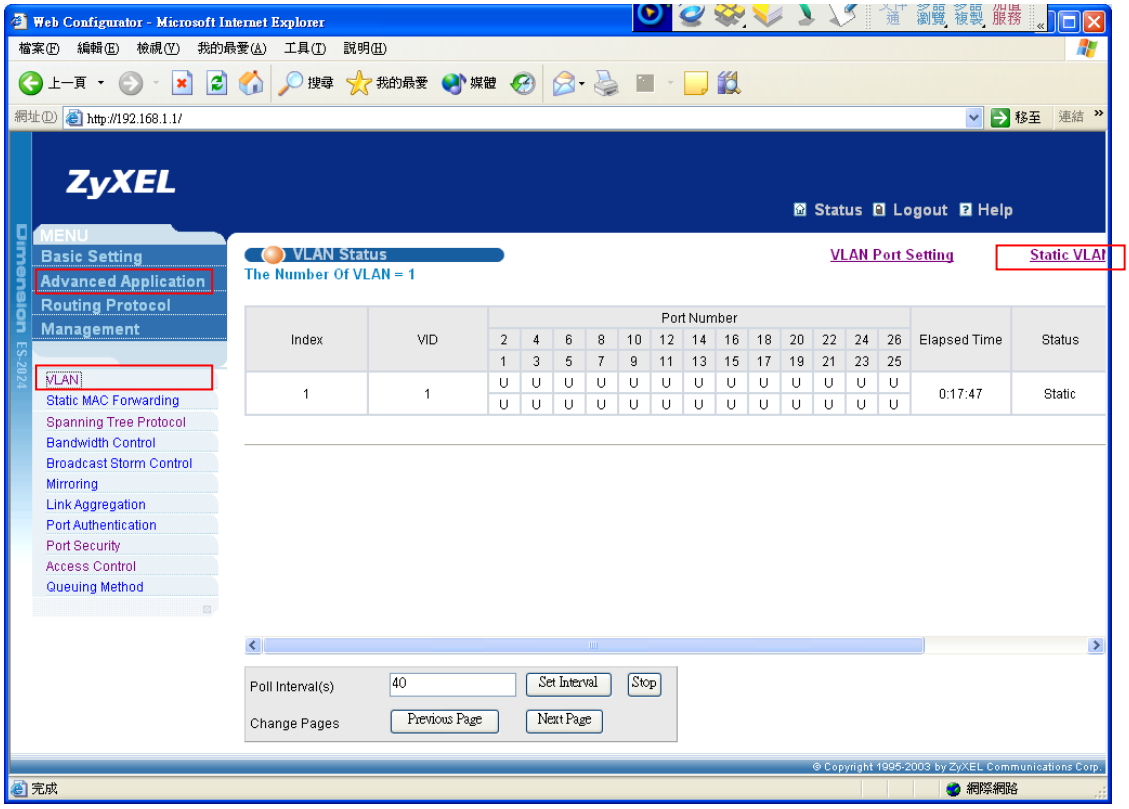
Make sure the VPI and VCI settings are the same as on the IES-5000 (the default is 0 and 34 respectively).



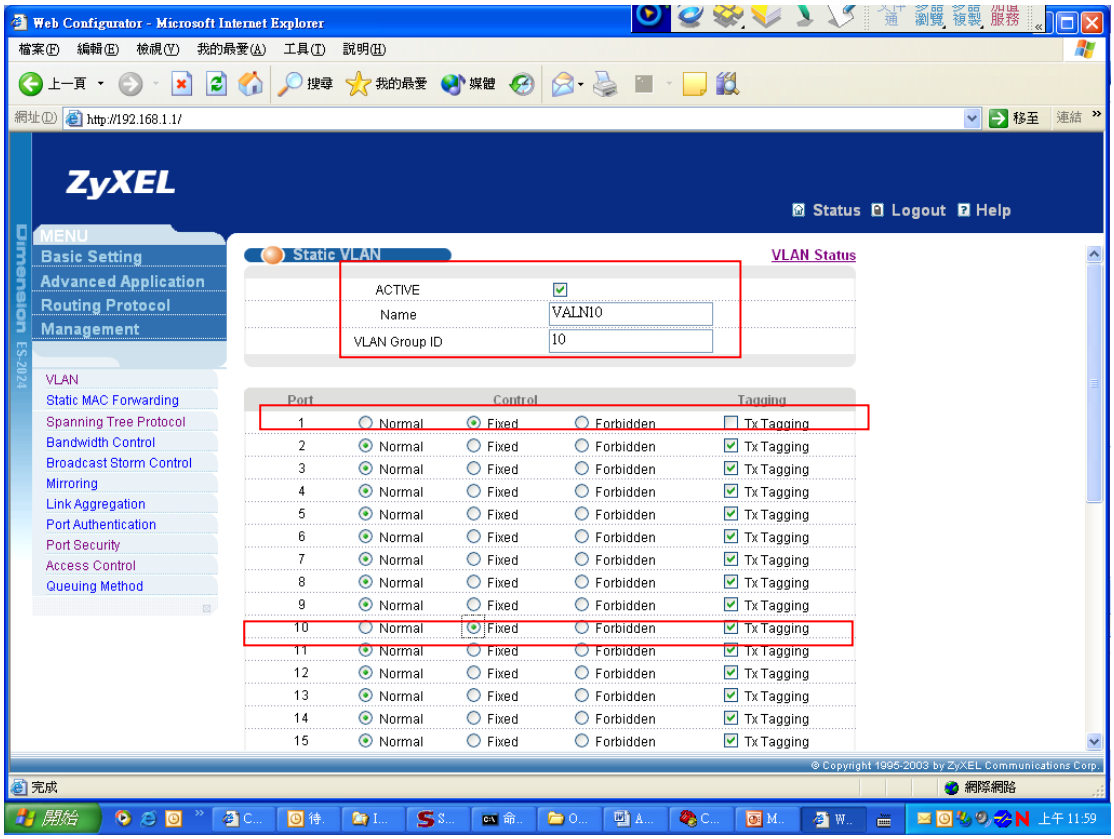
3. ES-2024 settings

3.1 VALN

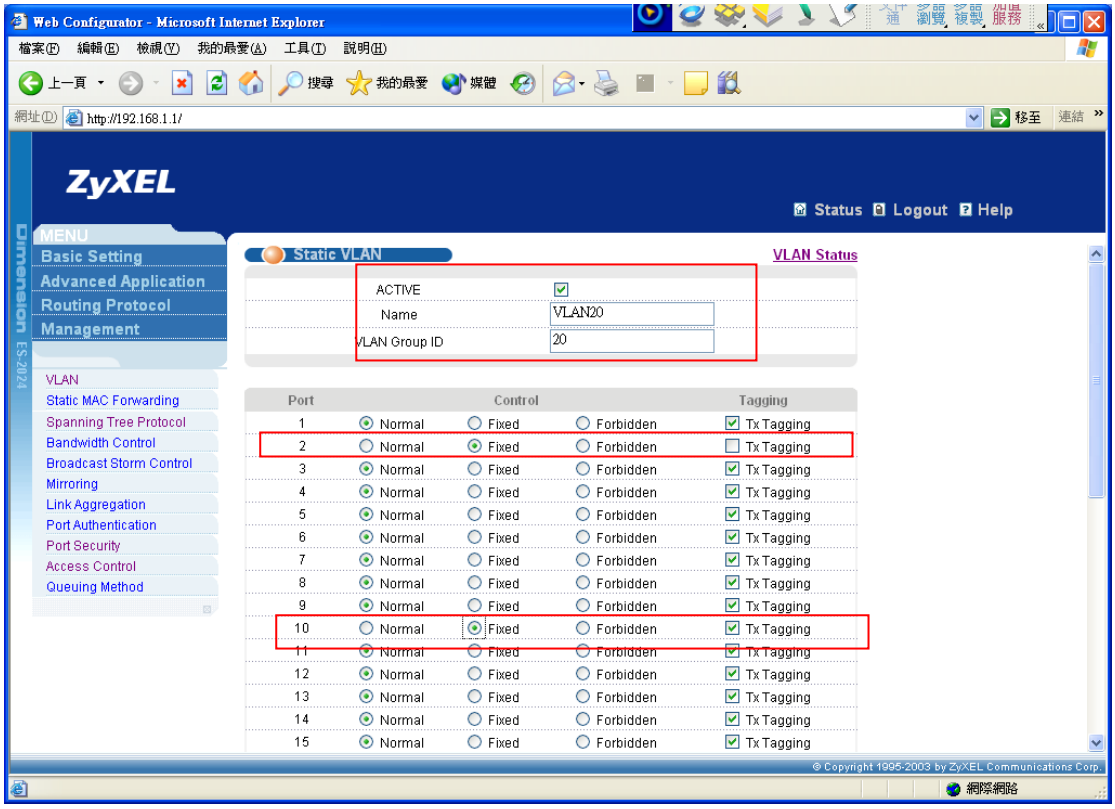
Click **Advanced Application** and **VLAN** in navigation panel to display the configuration screen as shown. Click **Static VLAN** to display the **Static VLAN** screen.



Create a VLAN with VID of 10. Assign ports 1 and 10 to be members of VLAN10. Select the **Tx Tagging** option to enable egress tagging on port 10.

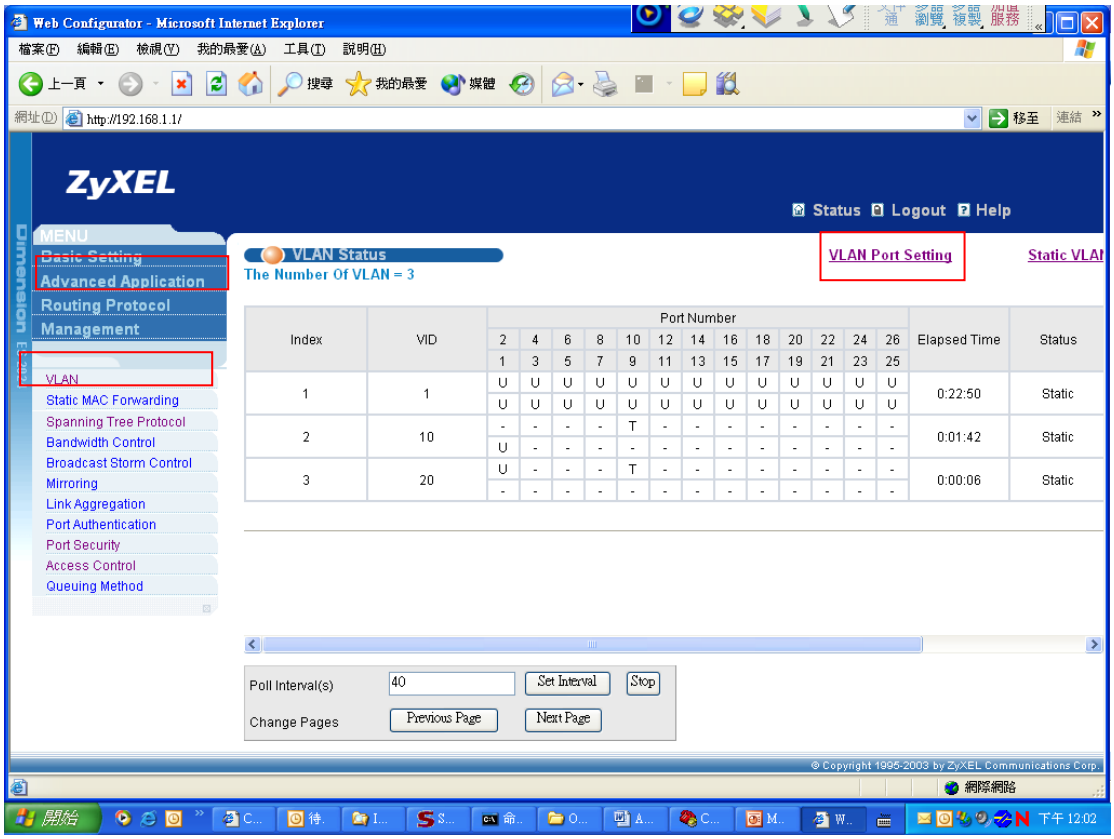


Create a VLAN with VID of 20. Assign ports 2 and 10 to be members of VLAN20. Select the **Tx Tagging** option to enable egress tagging on port 10.

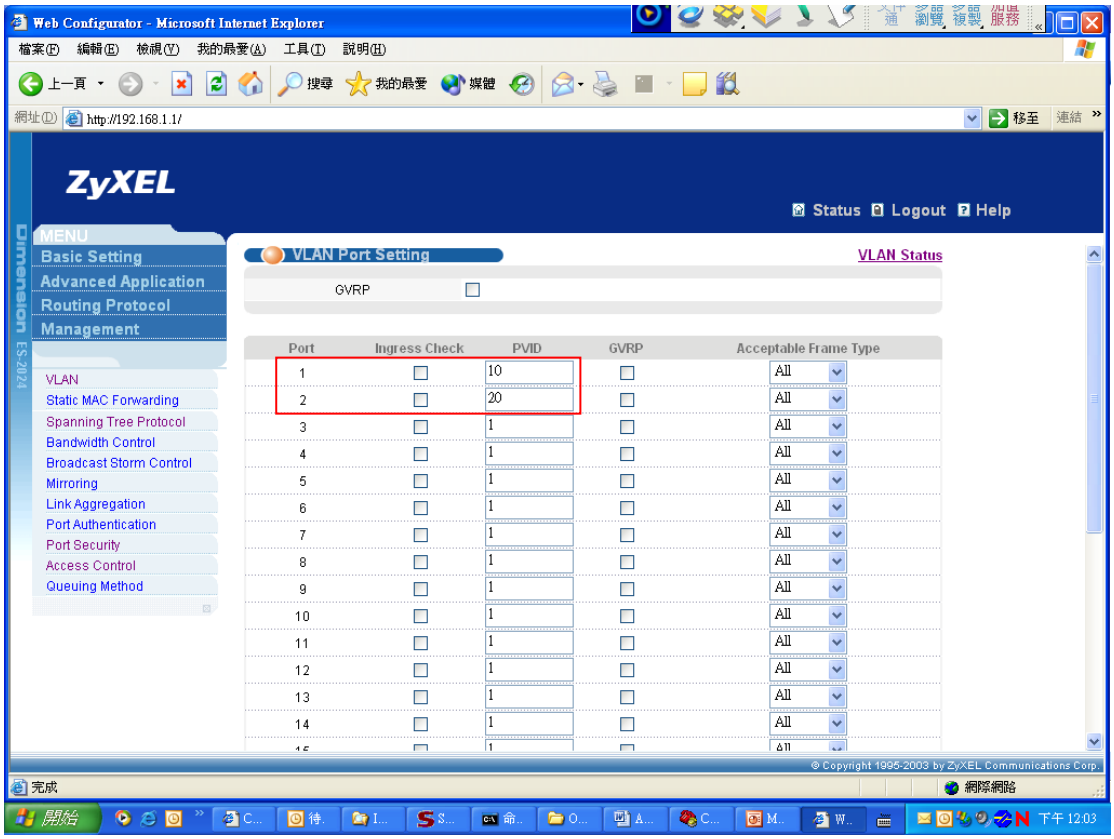


3.2 PVID setup

Click **Advanced Application** and **VLAN** in navigation panel to display the configuration screen as shown. Click **VLAN Port Setting** to show **VLAN Port Setting** screen.



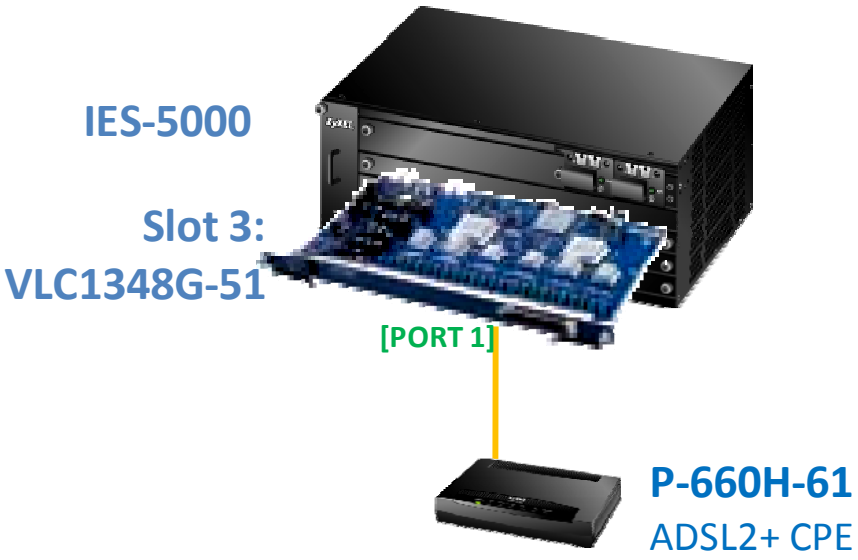
Set the PVIDs on port 1 and 2 to 10 and 20 respectively.



After the configuration on the devices are complete, video traffic will go through the 0/33 channel and the data traffic will go through the 0/34 channel. Since the 0/33 channel has a higher priority, video traffic will get processed and sent first if both traffic types arrive at the same time.

VDSL2 to ADSL2+ Fallback

The VLC1348G-51 can automatically use ADSL2+ for connections where VDSL2 training fails. This allows a longer connection distance. You can also specify ADSL2+ as the only protocol that can be used on the port connected to an ADSL2+ CPE.



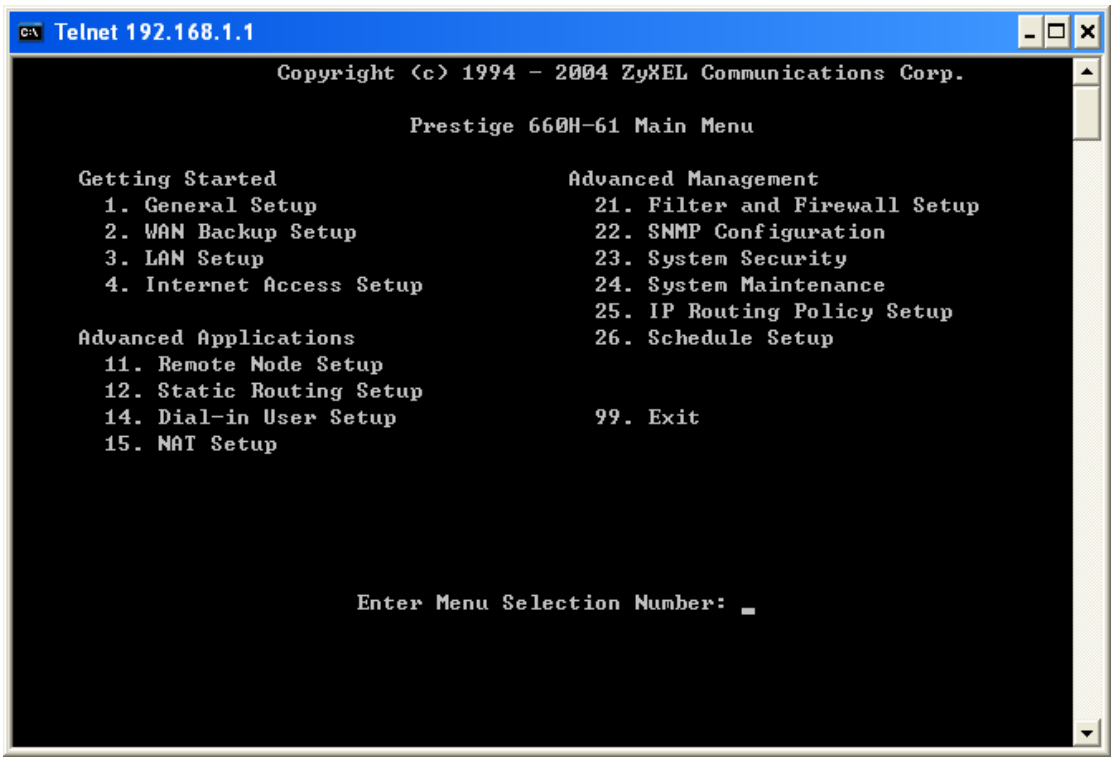
Configure the P-660H-61

1. Telnet into the P-660H-61

a. In Windows, click **Start** (usually in the bottom left corner), **Run** and then type “telnet 192.168.1.1” (the default IP address) and click **OK**.

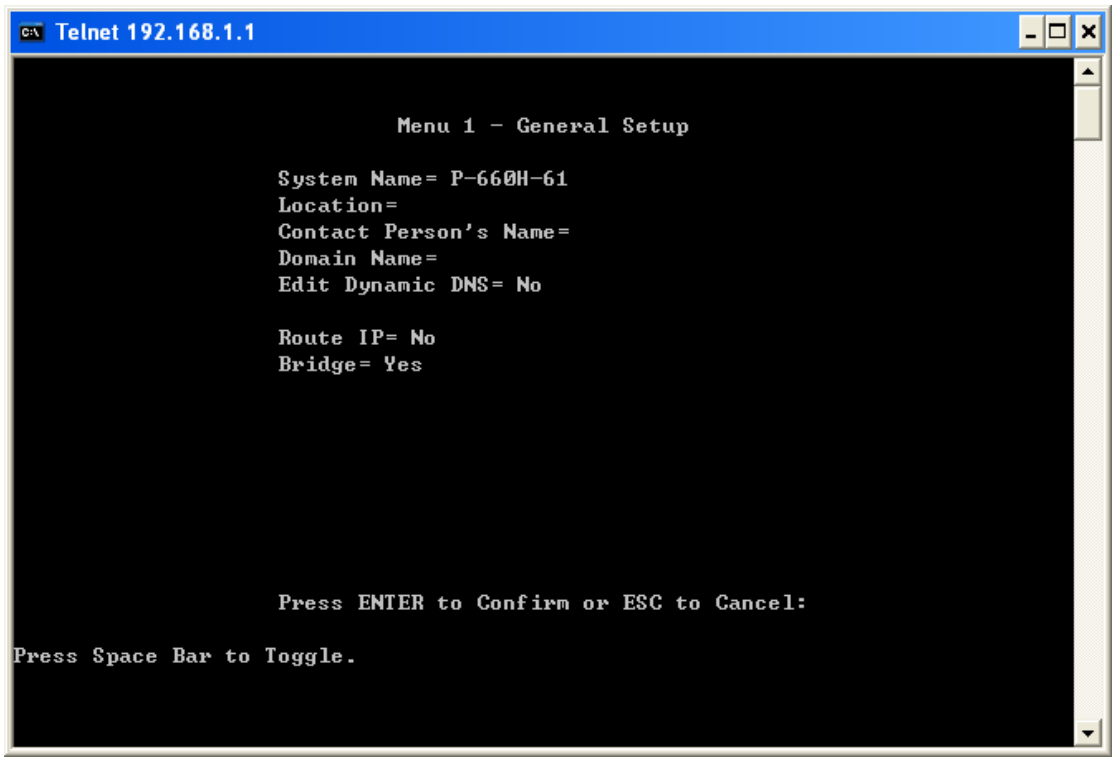
b. Enter “1234” in the **Password** field.

c. After entering the password you will see the main menu.



2. General Setup

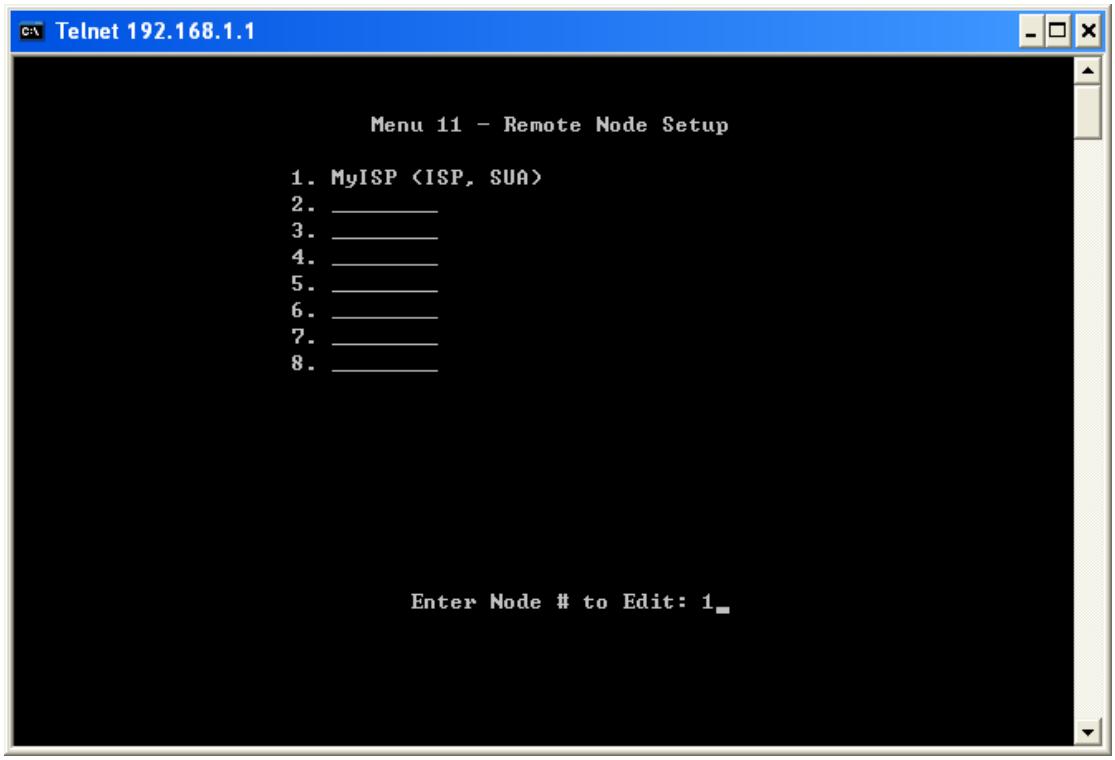
a. Enter **1** in the **Main Menu** to open **Menu 1 – General Setup**.
b. Type a name in the **System Name** field.
c. Select **No** in the **Route IP** field.
d. Select **Yes** in the **Bridge** field.
e. Press **ENTER** to confirm your changes.



3. Remote Node Setup

a. Enter **11** in the **Main Menu** to open **Menu 11 – Remote Node Setup**.

b. Enter **1** to configure the remote node of **MyISP (ISP, SUA)**.



c. **Menu 11.1 – Remote Node Profile** appears.

d. Select **Yes** in the **Active** field.

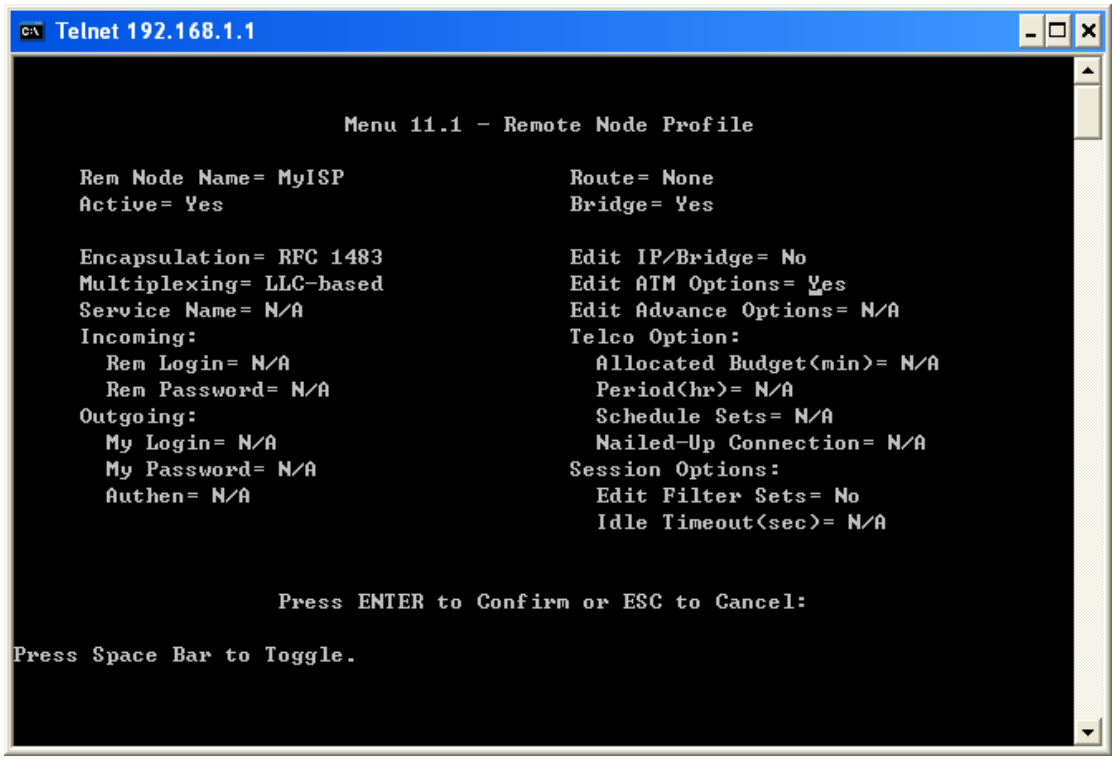
e. Select **RFC 1483** in the **Encapsulation** field.

f. Select **LLC-based** in the **Multiplexing** field.

g. Select **None** in the **Route** field.

h. Select **Yes** in the **Bridge** field.

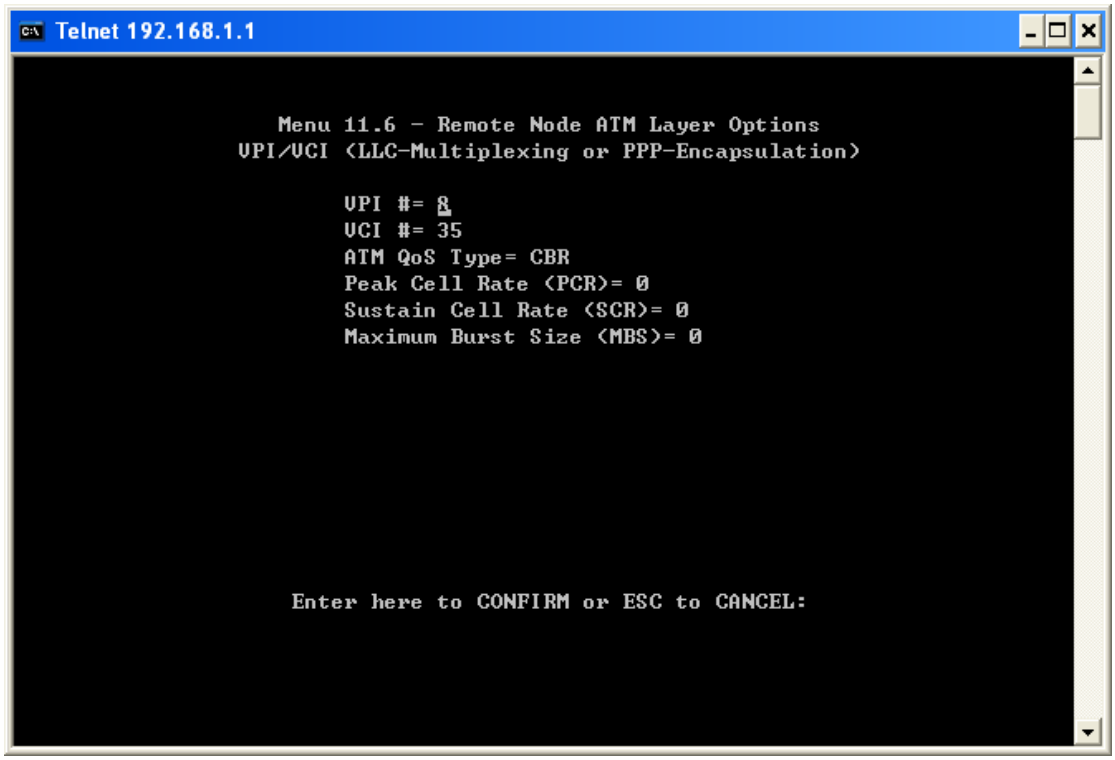
i. Select **Yes** in the **Edit ATM Options** field and press **ENTER** to display **Menu 11.6 – Remote Node ATM Layer Options**.



j. **Menu 11.6 – Remote Node ATM Layer Options** appears.

k. Specify VPI and VCI. In this case, we type **8** in the **VPI #** field and **35** in the **VCI #** field.

l. Press **ENTER** to confirm your changes.

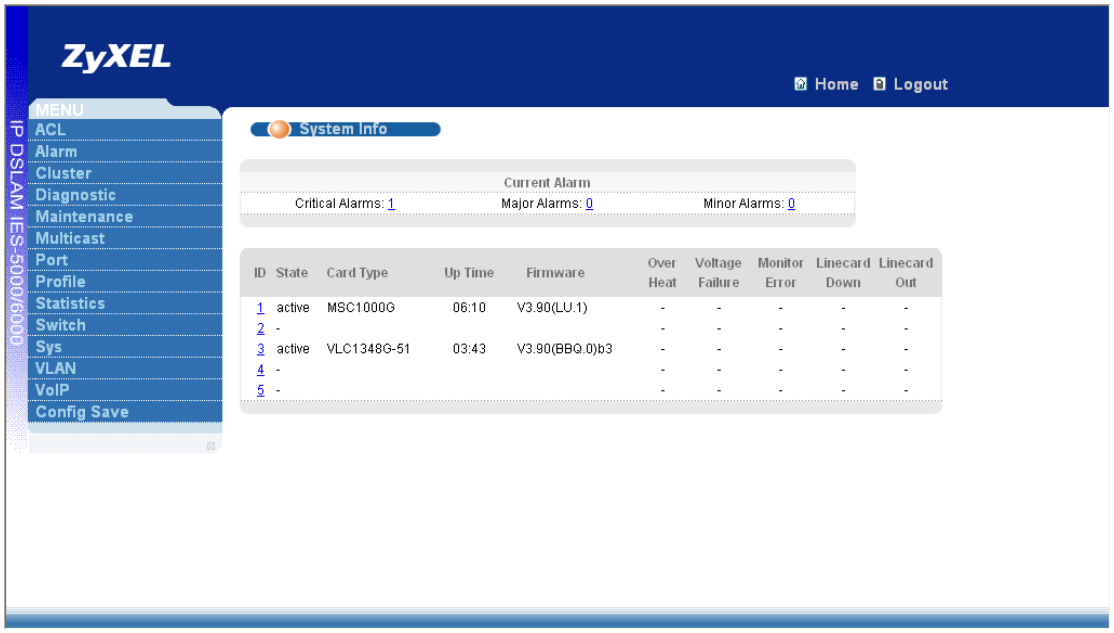


Configure the VLC1348G-51

1. Login

a. Connect to the IES-5000 via Internet browser. 192.168.1.1 is the default in-band management IP address and 192.168.0.1 is the default out-of-band (management port) IP address. Enter the default username (“admin”) and the password (“1234”) to access the device:

First web configurator screen appears.



2. VDSL Port Setup

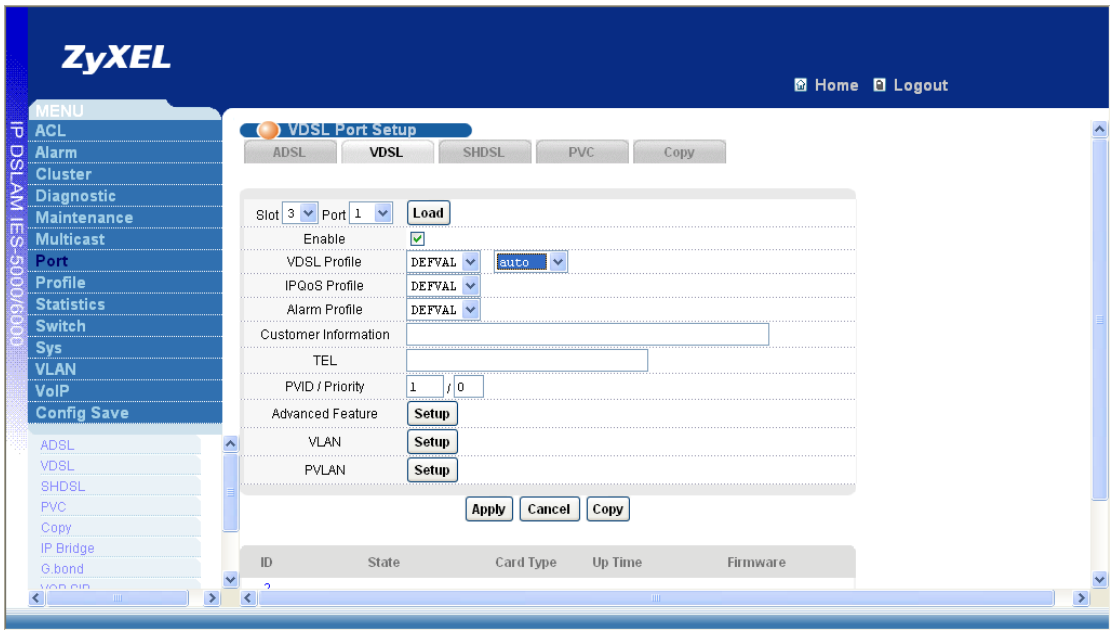
a. Click **Port** > **VDSL**.

b. Select slot **3** and port **1**, and click **Load** to display the settings as shown in this screen.

c. Select **Enable.**

d. Select **auto** from the second **VDSL Profile** drop-down list box to automatically detect the protocol used on the connected line.

e. Click **Apply**.

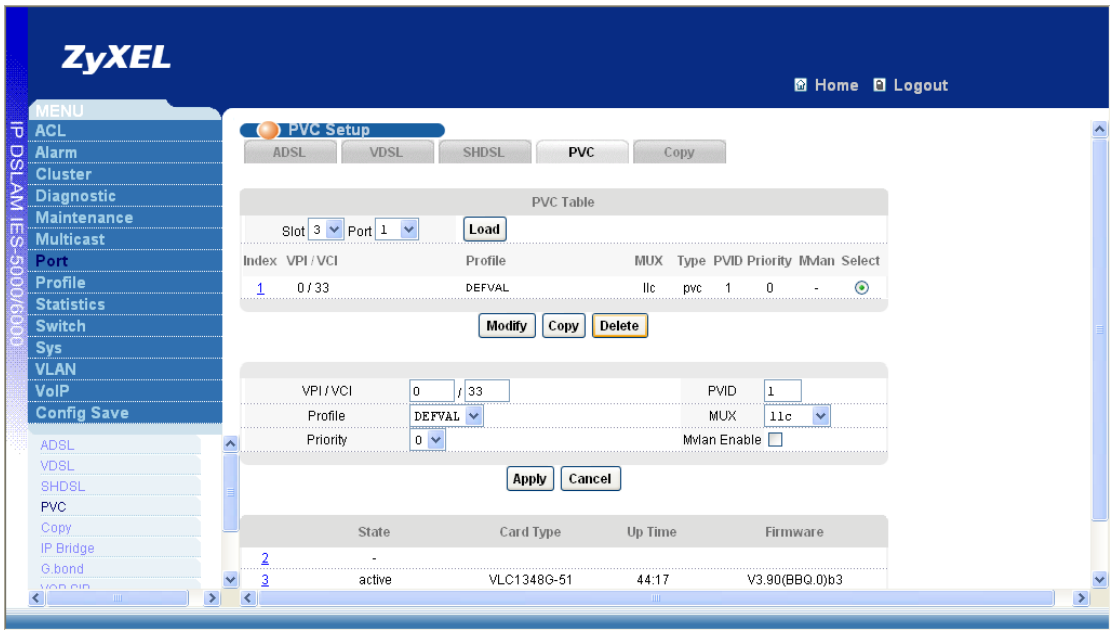


3. PVC Setup

a. Click **Port** > **PVC**.

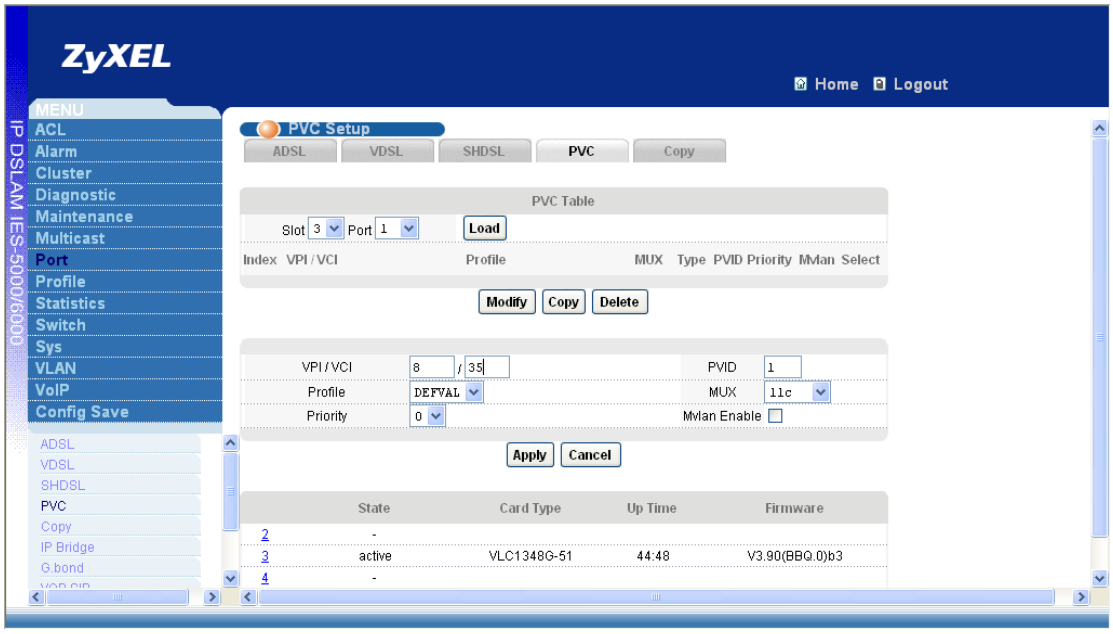
b. Select slot **3** and port **1**, and click **Load** to display the settings as shown in this screen.

c. Select index **1**, and click **Delete** to delete the default PVC (0/33).



d. Type **8/35** in the **VPI/VCI** field.

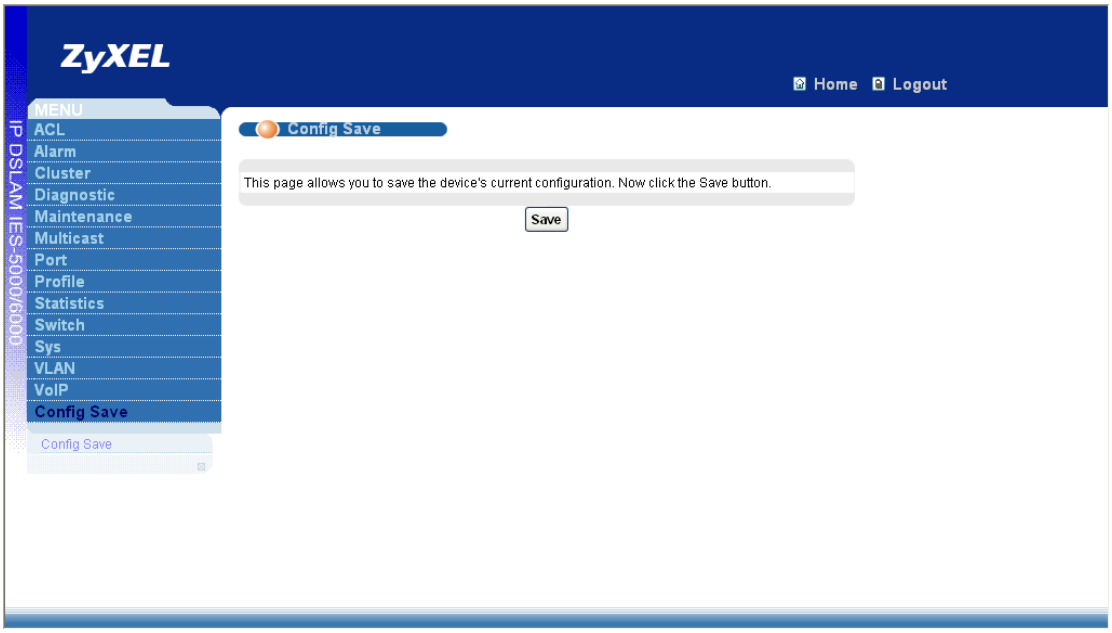
e. Click **Apply** to create the PVC.



4. Config save

a. Click **Config Save** on the navigation panel.

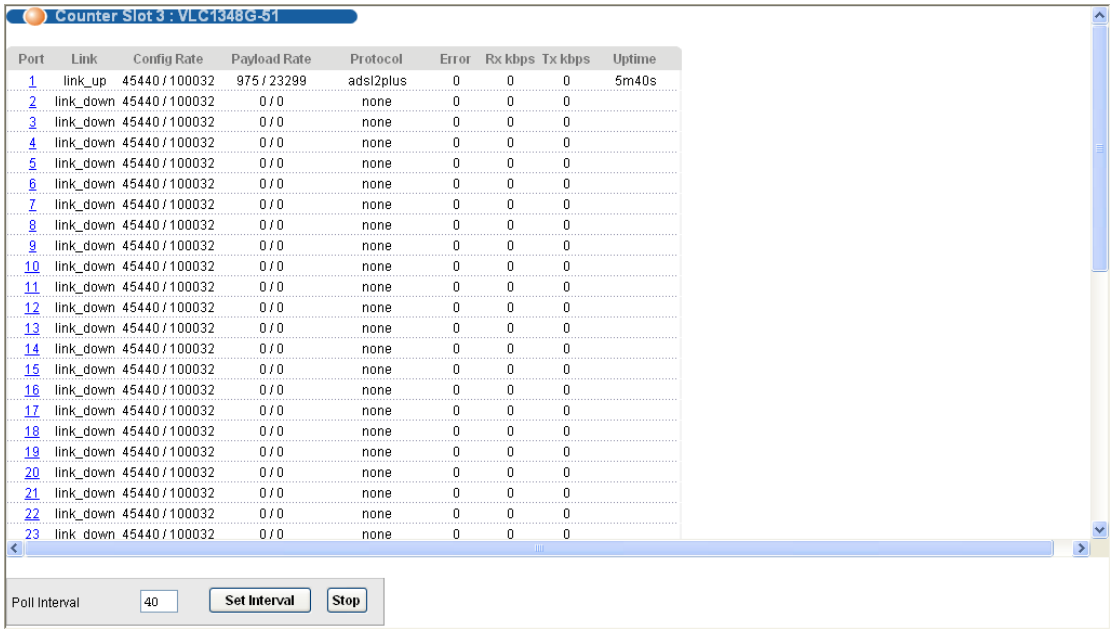
b. Click the **Save** button to save your configuration to nonvolatile memory.



5. Check status

a. Click **Statistics > Port Statistics**.

b. Click ID **3** to display the **Counter** screen. **Protocol** shows **adsl2plus** when port **1** is up.

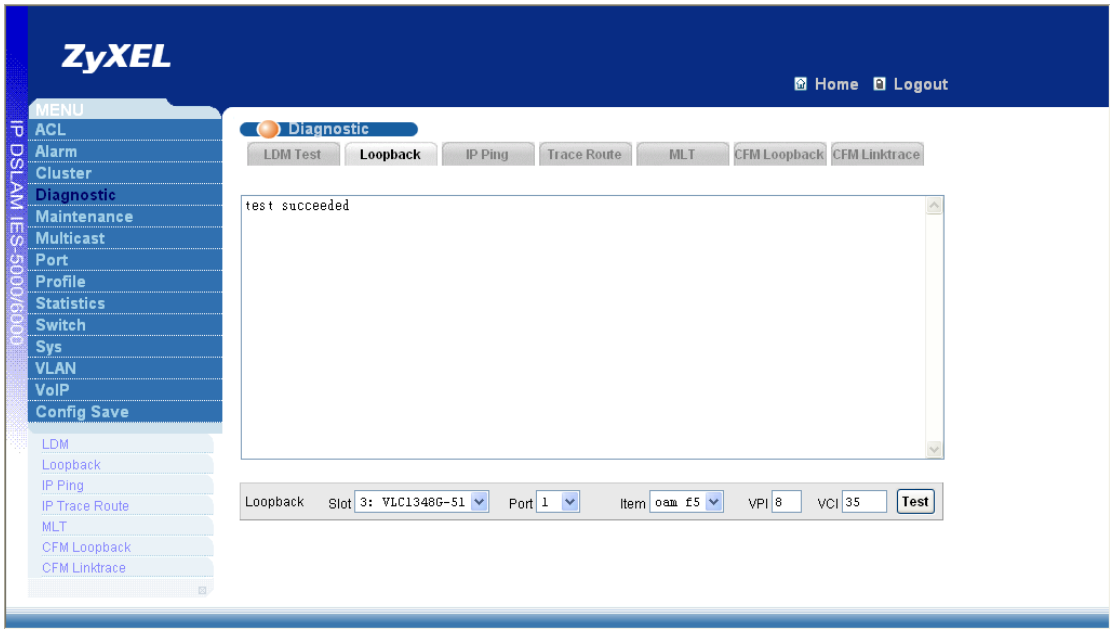


c. Click **Diagnostic > Loopback**.

d. Select port **1**.

e. Type **8** in VPI and **35** in VCI.

f. Click the **Test** button to perform an OAM F5 loopback test on port **1**.



Impulse Noise Protection (INP)

The impulse noise generator is required to prove the burst noise immunity of the VDSL transceiver. The noise shall consist of bursts of additive white Gaussian noise (AWGN) injected onto the line with sufficient power to ensure effective erasure of the data for the period of the burst, i.e., the bit error ratio during the burst shall be approximately 0.5 (assuming FEC is not applied). The noise burst shall be applied regularly at a repetition rate of at least 1 Hz. The duration of the burst is variable; at least values of 10, 50, 100, 250, and 500 μs shall be supported. The AWGN shall be generated with crest-factor of 5 and flat PSD up to 12 MHz, and further continuously declined with a roll-off equal to or steeper than 12 dB per octave. The PSD of the AWGN shall be variable in the range from –70 dBm/Hz to –140 dBm/Hz.

Interleaving shall be used to protect the data against bursts of errors by spreading the errors over a number of Reed-Solomon codewords. Interleaving can be programmable by software. Sudden strike noise can cause packet error. A buffer to protect ADSL Physical connection.

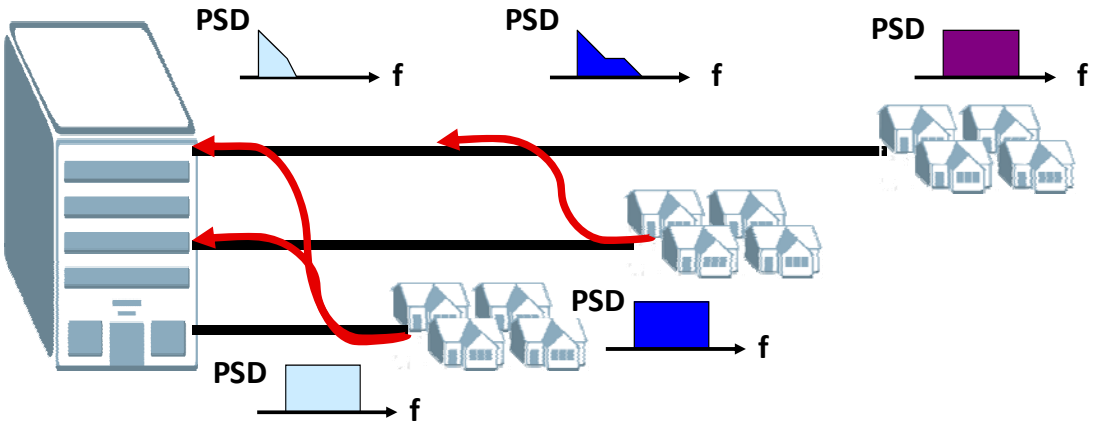
Error ratio during the burst shall be approximately 0.5 (assuming FEC is not applied). The noise burst shall be applied regularly at a repetition rate of at least 1 Hz. The duration of the burst is variable; at least values of 10, 50, 100, 250, and 500 μs shall be supported. The AWGN shall be generated with crest-factor of 5 and flat PSD up to 12 MHz, and further continuously declined with a roll-off equal to or steeper than 12 dB per octave. The PSD of the AWGN shall be variable in the range from –70 dBm/Hz to –140 dBm/Hz.

Upstream Power Back-Off (UPBO)

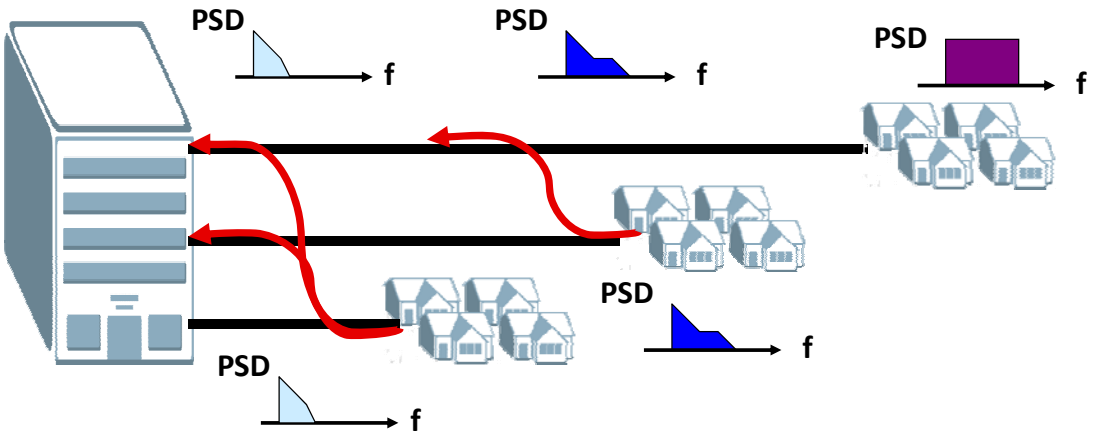
What is UPBO?

Upstream Power back-of (UPBO) helps to run services over loops with different length co-located in the same cable binder (“mixed length” deployments), especially in FEXT-dominated noise environment.

Strong FEXT generated by short loops can significantly degrade the performance of long loops if UPBO is not applied. On the other hand, UPBO reduces the transmit power of short loops and thus degrades their performance as well.



Enable UPBO to allow the system to adjust the transmit PSD of all lines based on a reference line length so that the PSD at the receiving end is the same.



The followings are general conclusions for applying UPBO in real network.

- **Non-FEXT dominated environment:**
  Do not apply UPBO!
  It only causes SNR reduction in short loops with no SNR improvement in long loops.
- **FEXT-dominated environment:**
  Apply UPBO for all loops shorter than the longest one!
  It always could be found an appropriate UPBO value avoiding any SNR reduction and even improving the SNR in either long or short loops (because of lower FEXT coupling in short loops).

Modes of UPBO

Defines the goal of the UPBO for the particular deployment. This goal usually allows avoiding performance degradation in some loops at expenses of another loops.
The appropriate mode for particular deployment is supposed to be set by the network operator. Standards should specify the recommended modes.

1. Protection of the long loop

Performance of the selected service over the selected Long loop is kept with no degradation (or with a controlled small degradation) relatively to the “equal length” scenario on the expense of shorter loops. Performance degradation for loops either shorter or longer that the Long loop are NOT restricted.

POZ: Doesn’t require any knowledge on the noise environment. The implementation is straightforward.
NEG: Protects actually only one loop (one dedicated service)

2. Equal maximum degradation for all loops

Loop of any length may be degraded relatively to the “equal length”scenario. The maximum value of degradation (usually expressed in SNR margin) is equal for all loops.

POZ: Penalizes all services equally (theoretically, by 3 dB of SNR margin).
NEG: Requires exact knowledge of the noise environment. The UPBO needs to be updated for any change in FEXT and non-FEXT (the worst case solutions for both usually brings rather poor results).

3. Improved performance of short loops

The goal of this mode is to maximize the performance of short loops keeping performance degradation of the Long loops limited.

NEG: Can be implemented for only one short loop. With more than one short loop performance degradation of long loops can't be limited.

4. Spectral mask compatibility with other services

A specific PSD mask is specified for each loop length with no reference on the performance degradation in the particular loop. The initial definition of PSD mask could be based on any of the modes 1-3 or on spectral compatibility with other xDSL.

POZ: Predicts all spectral compatibility problems with existing and future services. Selected as the UPBO mode in ITU.
NOTE: The exact implementation technique for this method is under discussion.

Methods of UPBO

Method of UPBO specifies how to reach the goal defined by the mode. Sometimes the same goal could be reached by different methods. Compatibility of different methods should be taken in account. The following PBO methods are widely discussed:

- Reference PSD
- Reference Length
- Multiple Reference Length
- Equalized FEXT
- Reference Frequency
- Reference Noise

802.1ag CFM

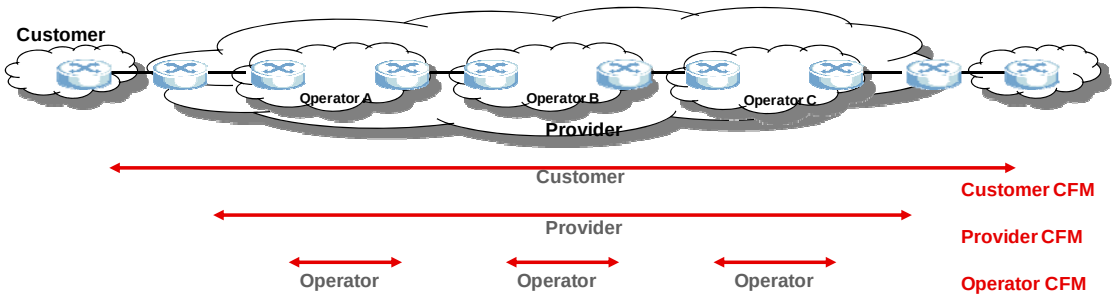
What is CFM?

IEEE 802.1ag Connectivity Fault Management (CFM) allows service providers to manage each customer service instance individually. A customer service instance, or Ethernet Virtual Connection (EVC),is the service that is sold to a customer and is designated by the Service-VLAN tag. Hence,802.1ag operates on a per-Service-VLAN (or per-EVC) basis. It enables the service provider to know if an EVC has failed, if so, provides the tool to enable rapid isolation of the failure.

This function would be absolutely critical in the following scenarios:

1. A SNMP trap indicates a fault has occurred in the network. How does the service provider know exactly which customers are affected, particularly if there are complex failover mechanisms in place?
2. An instance has failed. How does the service provider discover this?
3. A link or devices in an instance fails. How do the other devices find out so they can reroute around the failure.
4. An instance was just installed. How does the service provider confirm that it is operational?

802.1ag providers the tools to do all of the above easily and quickly, thus reducing operating costs, increasing availability.



- Customer detects failure: diagnose and isolate the failure, report to providers
- Provide detects failure: diagnose and isolate the failure, report to operators
- Operator detects failure: diagnose and find out root causes
- MS: Management System

Often there are three different organizations involved in a Metro Ethernet service: customers, service providers, and operators. Customers purchase Ethernet service from service providers. Service providers may use their own networks, or the networks of other operators to provide connectivity for the requested service. Customer themselves may be service providers, for example, a customer may be an Internet service provider that sells Internet connectivity.

CFM Terms

- **MD--Maintenance Domain**
  - An MD is a group identified by a level number.
  - There are 8 MD Levels, 0-7; the wider the physical extent, the higher MD Level number.

You can create more than one MA in one MD.

MD Levels	7	6	5	4	3	2	1	0
	Customer			Provider		Operator		

A maintenance domain is an administrative domain for the purpose of managing and administering a network. A domain is assigned a unique maintenance level by the administrator, which is useful for defining the hierarchical relationship of domains. MD may nest or touch, but cannot intersect. If two domains nest, the outer domain must have a higher maintenance level than the one it involves.

- **MA--Maintenance Association**
  - An MA is a group identified by a VLAN ID.
  - One MA should belong to one and only one MD group.

- **MEP--Maintenance End point**
  - An MEP port has the ability to send and reply the CCMs, LBMs and LTMs. It also gets other MEP port information from neighbor switches' CCMs in an MA.

An MEP port has the ability to send and reply the CCMs, LBMs and LTMs. It also gets other MEP port information from neighbor switches' CCMs in an MA.

CCM—Continuity Check Message

LBM—Loop Back Message

LTM—Link Trace Message

- **MIP--Maintenance Intermediate Point**
  - o An MIP port forwards the CCMs, LBMs, and LTMs and replies the LBMs and LTMs by sending LBRs and LTRs.

An MIP port forwards the CCMs, LBMs, and LTMs and replies the LBMs and LTMs by sending LBRs and LTRs.

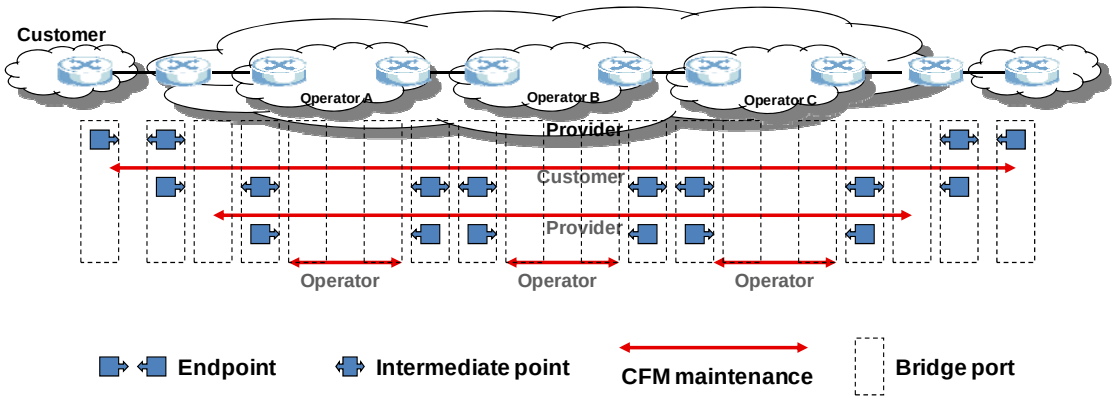
CCM—Continuity Check Message

LBM—Loop Back Message

LTM—Link Trace Message

LBR—Loop Back Response

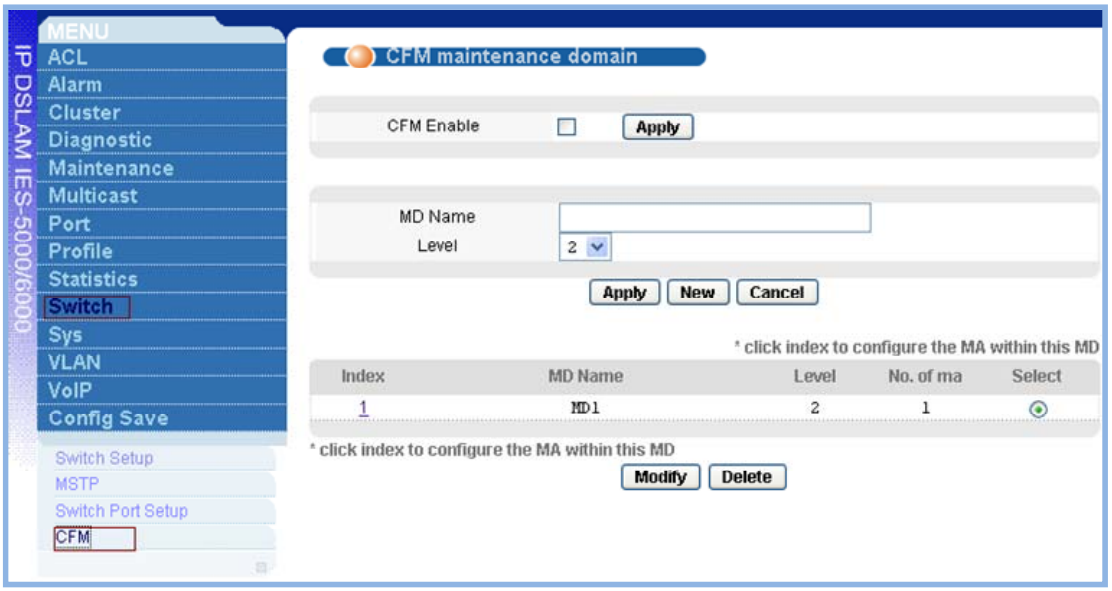
LTR—Loop Trace Response



Any port of a bridge is referred to as a maintenance point which may be classified as either a maintenance endpoint, maintenance intermediate point. Maintenance endpoints reside at the edge of a maintenance domain, whereas maintenance intermediate points are internal to the domain. Each maintenance endpoint is assigned an unique id within its domain.

WEB GUI Introduction

1. CFM MD Screen

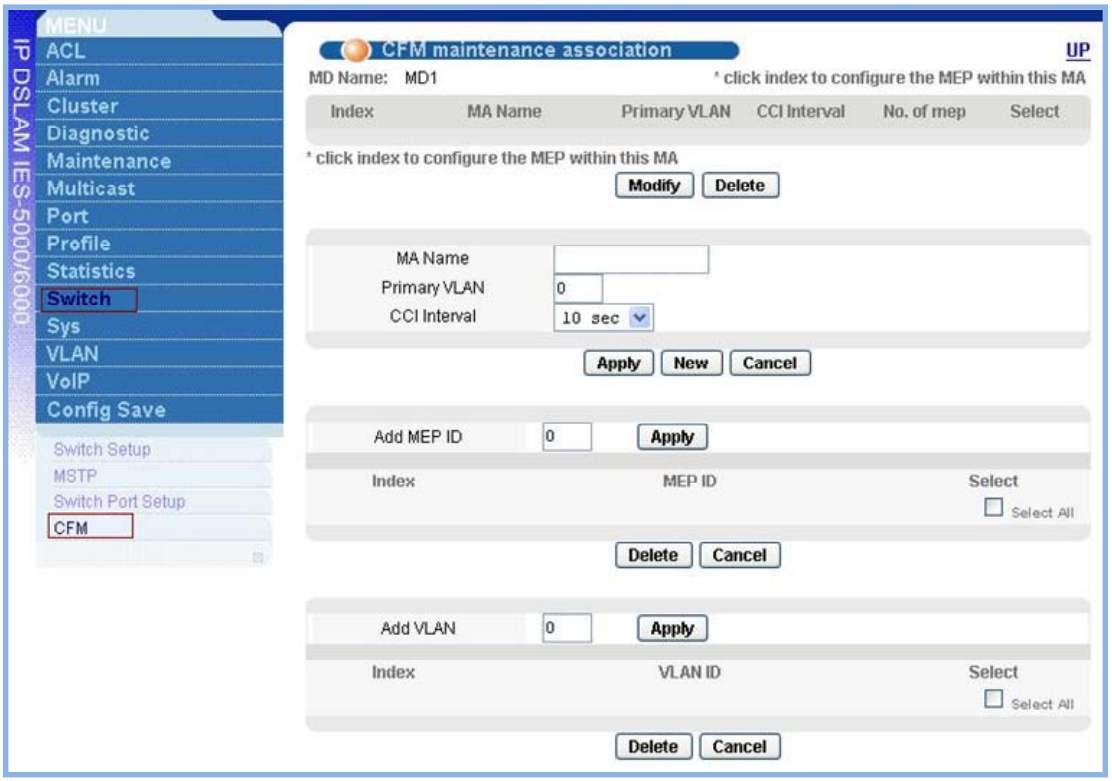


CFM Enable: Select or deselect the check box and click Apply to turn the CFM feature on or off.

MD Name: Type a name (up to 31 printable ACSII characters) for this MD. This is for the purpose of identification.

Level: Type a level number (0~7) for this MD.

2. CFM MA Screen



MA Name: Type a name (up to 15 printable ACSII characters) for this MA. This is for identification purpose.

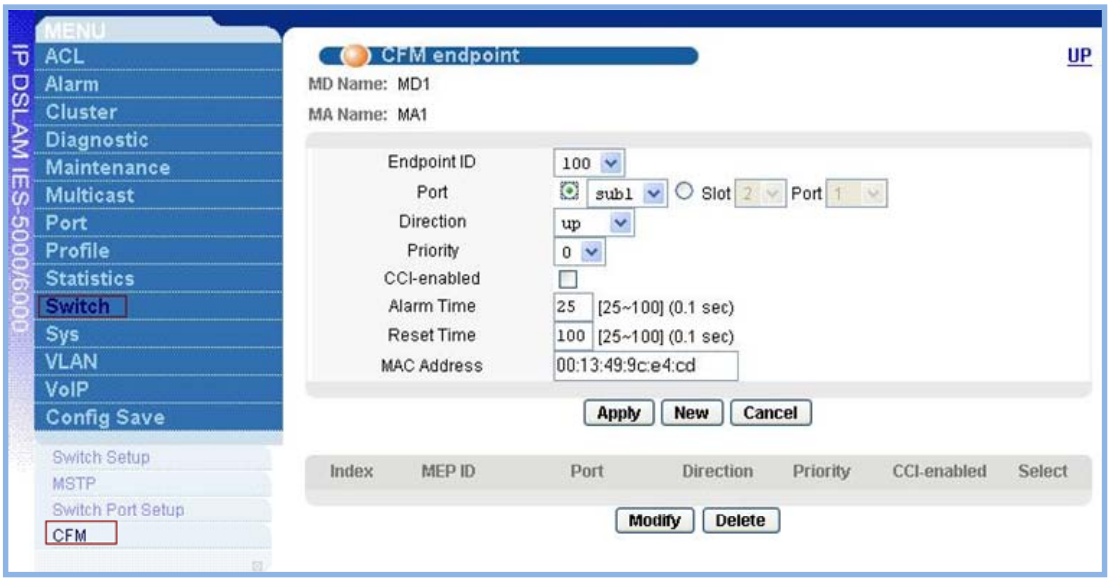
Primary VLAN: Type the primary VLAN ID (1~4094).

CCI Interval: Select a number to specify how often the device sends a Continuity Check Message. (1 sec/10 sec/60 sec/10 min)

Add MEP ID: Enter a remote MEP ID (1~8191) associated to this MA and allowed to be used in the CFM test.

Add VLAN ID: Enter a VLAN ID (1~4094) associated to this MA

3. CFM MEP Screen



Endpoint ID: Select a valid MEP ID which is defined in the CFM maintenance association screen.

Port: This binds the MEP ID to a physical port on the device. You can select an Ethernet port or a DSL port.

Direction: Select whether to send CCMs (Continuity Check Messages) from the end point you selected in this screen (**down**) or from another active Ethernet port (**up**).Select up only when the link of the specified end point is down.

Priority: Select the priority level for the CCMs configured in this screen. “0” is the lowest priority and “7” is the highest.

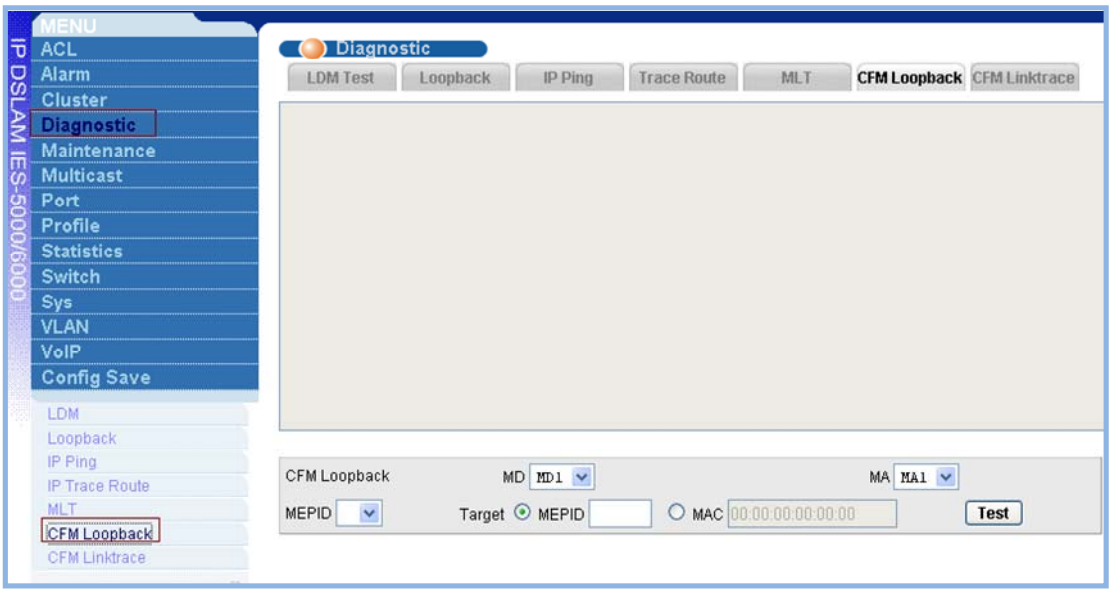
CCI-enabled: Select this to enable CCMs sending from the end point configured in this screen. Deselect this to stop CCMs sending.

Alarm Time: This is the number of seconds the ZyXEL Device waits to send a local alarm after three CFM_ERROR events have been defected.

Reset Time: This is the number of seconds the ZyXEL Device waits to cancel a local alarm after a CFM_ERROR event has been resolved and no other alarms occurred.

Mac Address: Enter the CFM en point’s MAC address.

4. Loopback Diagnosis



MD: Select an MD name.

MA: Select an MA name under the selected MD.

MEPID: Select an MEP ID to specify which MEP port on the device initiates the test.

Target: Specify the destination of the link you are checking. You can select **MEPID** and enter a remote MEP's ID or select **MAC** and enter a remote MEP port's MAC address.

Test: Click this to start the loopback connectivity test.

CLI Command Introduction

- **Enable CFM**

  MSC1000G> switch cfm enable

- **Disable CFM**

  MSC1000G>swtichcfm disable

- **Create a MD**

MSC1000G> switch cfmmd set <md-name><level>

- **Delete a MD**

MSC1000G> switch cfmmd delete <md-name>

- **Create a MA**

MSC1000G> switch cfm ma set <md-name><ma-name><primary-vlan> [<cci-interval>]

- **Delete a MA**

MSC1000G> switch cfm ma delete <md-name><ma-name>

- **Create a MEP**

MSC1000G> switch cfmmep set
<md-name><ma-name><mep-id><giga-port>|<slot-port><direction><priority>
[cci<cci-enabled>] [alm<alarm-time>] [rst<reset-time>] [mac<mac-address>]

- **Delete a MEP**

MSC1000G> switch cfmmep delete <md-name><ma-name><mep-id>

- **Create a MIP**

MSC1000G> switch cfmmip set <md-name><ma-name><giga-port>|<slot-port>

- **Delete a MIP**

MSC1000G> switch cfmmip delete <md-name><ma-name><giga-port>|<slot-port>

- **Execute Loopback**

MSC1000G> diagnostic cfm loopback <md-name><ma-name><ep-id><remote-ep-id>|<mac>

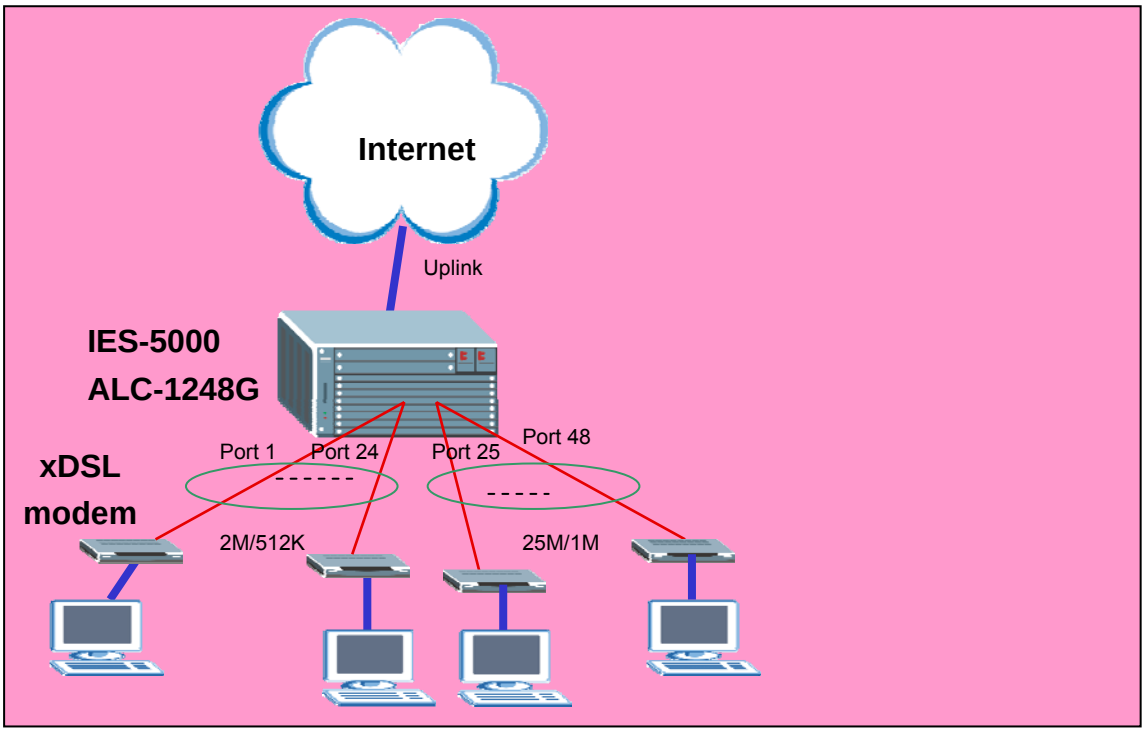
- **Execute Linktrace**

MSC1000G> diagnostic cfmlinktrace set

<md-name><ma-name><ep-id><remote-ep-id>|<mac><ttl>

Setting up different DSL port speeds to different subscribers

An ISP may want to configure a different line speeds for each DSL port. This can be easily and efficiently done in the ZyXEL IES-5000 using profiles. You can configure line profiles with different parameter settings based on the user requirements and apply the profile to one or more subscriber ports.
In this application example, we will show you how to create two profiles - one for low speed requirements with an upstream/downstream bandwidth of 2M/512Kbps and the other for high speed requirements with an upstream/downstream bandwidth of 25M/1Mbps.
For this example, you want to provide low line speed to subscribers on ports 1 to 24 and high line speed to business subscribers on ports 25 to 48.



Configuring and applying the profiles to subscriber ports
For this example, we will use configure the profile on an IES-5000 that connects to ADSL CPEs (ZyXEL Prestige 660R-61).

1. IES-5000

1.1 Profile Setup

Configure a profile to set low line speed. Enter a descriptive name for this profile (for example, “Profile_LowSpeed”) and set the maximum upstream and downstream rates (for example, 512Kbps and 2048Kbps).

Similarly, configure a profile to allow a high line speed. Enter a descriptive name for the profile (for example, “Profile_HighSpeed”) and set the maximum upstream and downstream rates (for example, 1280Kbps and 24992Kbps).

Configuration example using the CLI:

a.)High Speed (1M/24M) profile setup:
MSG1000G> profile adsl set 1_24M 1024 24576 minrate 64 64 delay 20 20 usmgn 310 0 60 dsmgn 310 0 60 usra startup 90 30 dsra startup 90 30

b.) Low Speed (512k/2M) profile setup:
MSG1000G> profile adsl set 512_2M 512 2048 minrate 64 64 delay 20 20 usmgn 310 0 60 dsmgn 310 0 60 usra fixed 90 30 dsra startup 90 30

Save current configuration
MSG1000G> config save

1.2 Profile Assignment

Select and assign Profile_LowSpeed to port 1. After setting port 1, copy the settings of port 1 to ports 2 to 24.

Assign Profile_HighSpeed to port 25. You also can set the port to use the ADSL2+ mode. Then, similarly, copy the settings of port 25 to the ports 26 to 48.

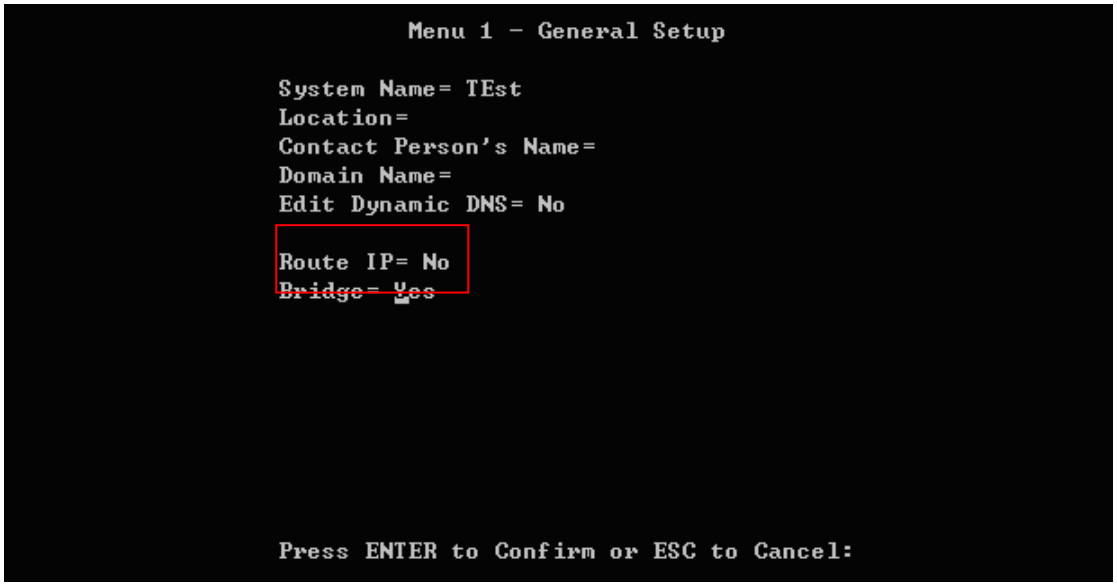
CI command:
MSG1000G> port adsl set 7-1~24 512_2M auto
MSG1000G> port adsl set 7-25~48 1_24M auto
MSG1000G> port enable 7-1~48
MSG1000G> port pvc set 7-1~48-0/33 DEFVAL llc 1 0
MSG1000G> config save

2. Prestige 660R-61

Next configure the CPE device. Set the Prestige 660R-61 to work in bridge mode using the VPI/VCI settings of 0/33 (the default on IES-5000). Since the Prestige 660R-61 has a built-in telnet server, you can telnet and log into the management interface.

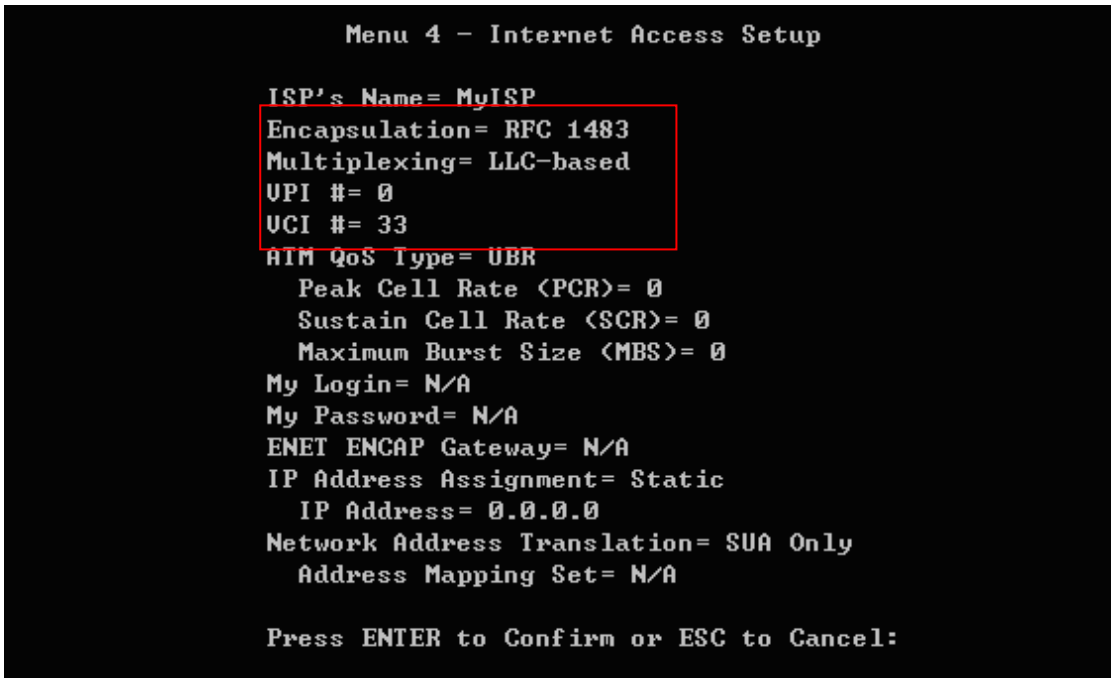
2.1 Menu 1: General Setup

Go to Menu 1 to set the Prestige 660R-61 in bridge mode. In this menu, select **No** in the **Route IP** field and **Yes** in the **Bridge** field.



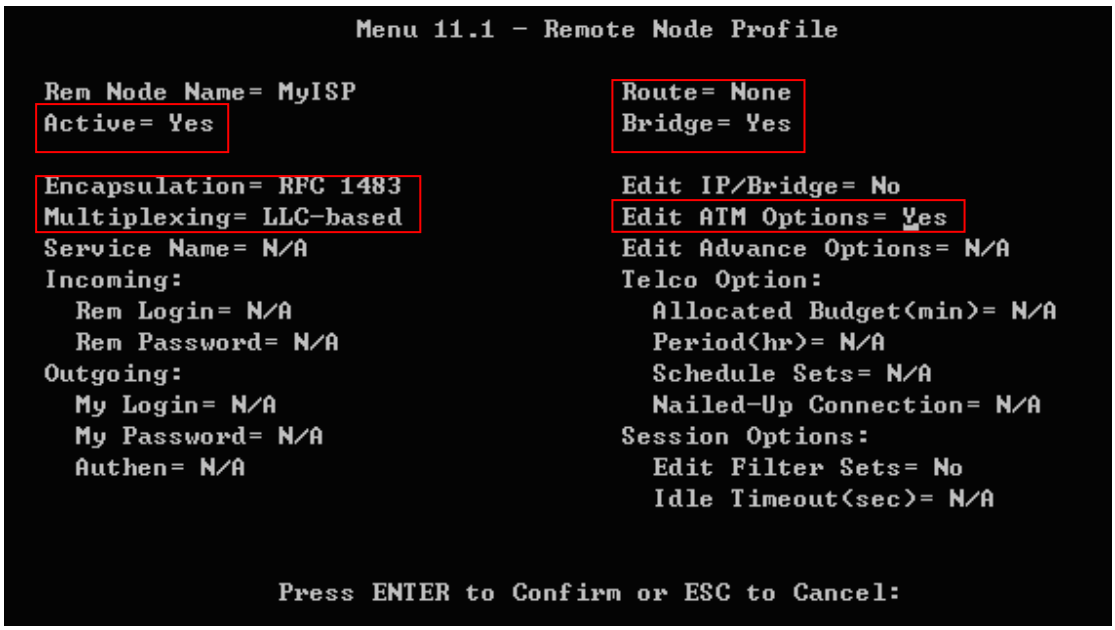
2.2 Menu 4: Internet Access Setup

For bridge mode, select **RFC 1483** in the **Encapsulation** field with **LLC-based** multiplexing. Also set the Prestige to use the same VPI and VCI settings as the IES-5000 (the default is 0 and 33 respectively).



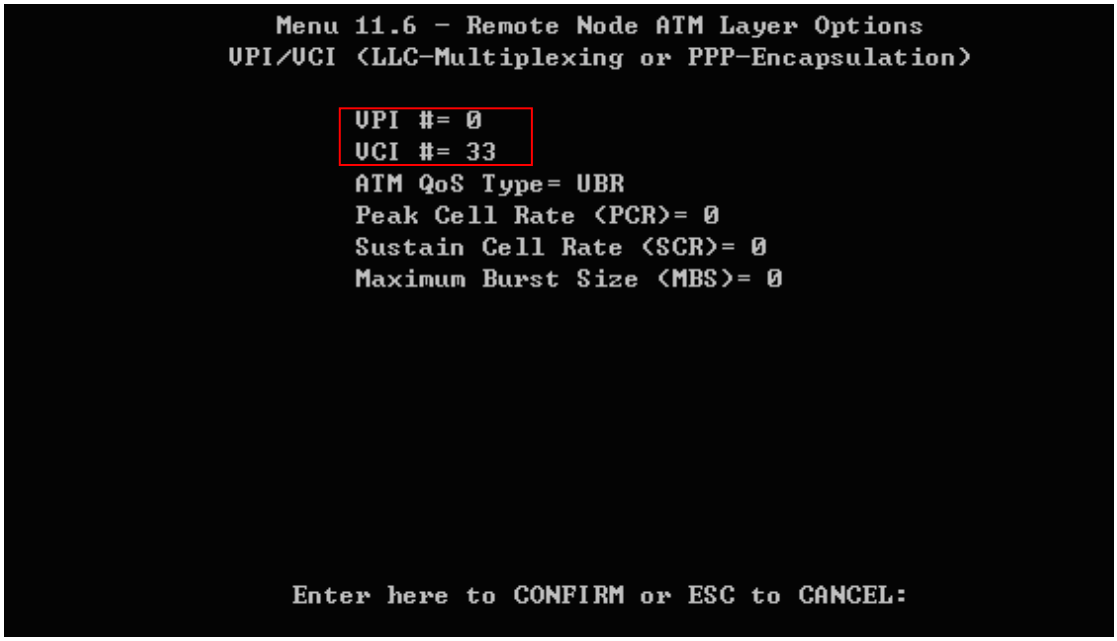
2.3 Menu11.1: Remote Node Profile

In menu 11.1, select Yes in the Active field to activate this remote node profile. Make sure the encapsulation and multiplexing settings are the same as in menu 4. Select Yes in the Edit ATM Options field and press [ENTER] to enter menu 11.6.



2.4 Menu11.6: Remote Node ATM Layer Options

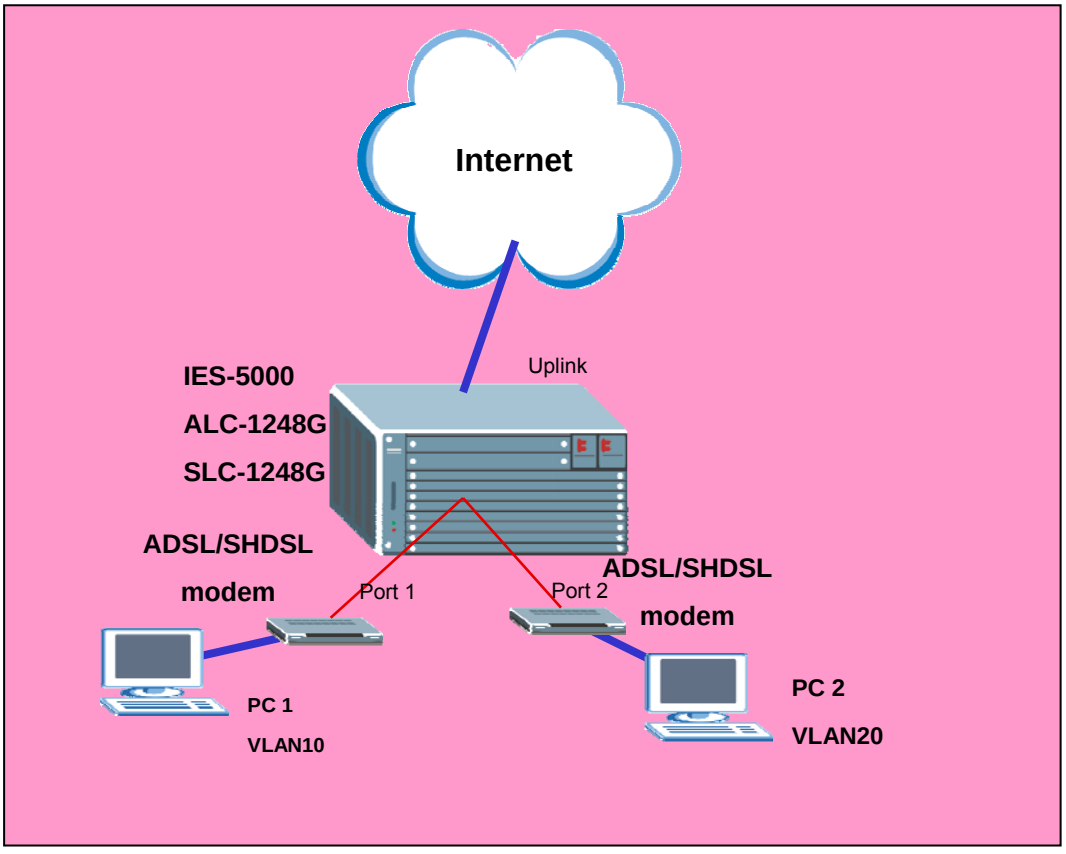
Make sure the VPI and VCI settings are the same as on the IES-5000 (the default is 0 and 33 respectively).



Configuring 802.1Q VLAN

A VLAN (Virtual Area Network) allows a physical network to be partitioned into multiple logical networks. Stations on a logical network belong to one group called VLAN group. A station can belong to more than one group. The stations on the same VLAN group can communicate with each other. With VLAN, a station cannot directly talk to or hear from stations that are not in the same VLAN groups.

In this application, we will show you how to configure an 802.1q VLAN. The following figure shows a VLAN network example where two computers (PC1 and PC2) are connected to ports 1 and 2 on the line card. Each computer belongs to a different VLAN (VLANs 10 and 20). Therefore the computers cannot communicate directly to each other. However, PC1 and PC2 still need connection to the Internet.



Setting up a VLAN

For this application, we will use an IES-5000 and Prestige ADSL 660R-61 CPE (any DSL CPE or P791 if you have the SLC-1248G line card installed on the IES). Since the two ports belonging to different VLANs need Internet access via the Uplink port

on the IES-5000, another VLAN (to which the two ports are a member of) need to be configured.

1. IES-5000 Settings

1.1 VLAN settings

Create a VLAN group with VID 10 and set Port 1, ENET1 and ENET2 to be members of this VLAN.

CI command:

TGE1> vlan set 10 up1 fix untag
TGE1> vlan set 10 up2 fix untag
TGE1> vlan name 10 VLAN10
TGE1> port pvc vlan 7-1-0/33 10 join untag

Create a VLAN group with VID 20 and set Port 2, ENET1 and ENET2 to be members of this VLAN.

CI command:

TGE1> vlan name 20 VLAN20
TGE1> vlan set 20 up1 fix untag
TGE1> vlan set 20 up2 fix untag
TGE1> port pvc vlan 7-2-0/33 20 join untag

Create a VLAN group with VID 200 and set slot 7, Port 1, Port 2, ENET1 and ENET2 to be members of this VLAN.

CI command:
TGE1> vlan name 200 VLAN200
TGE1> vlan set 200 up1 fix untag
TGE1> vlan set 200 up2 fix untag
TGE1> port pvc vlan 7-1-0/33 200 join untag
TGE1> port pvc vlan 7-2-0/33 200 join untag

1.2 PVID settings

After creating the three VLANs, you need to set the PVID on the ports.

For this example, assign VLAN 200(PVID) to ENET1 and ENET2. Also, assign VLAN 10 and VLAN 20 to Port1 and port2 respectively.

CI command:

TGE1> switch port pvid up1 200
TGE1> switch port pvid up2 200
TGE1> port pvc set 7-1-0/33 DEFVAL llc 10 0
TGE1> port pvc set 7-2-0/33 DEFVAL llc 20 0

1.3 Port Isolation

On the IES-5000, you can isolate ports without configuring VLAN groups in the CLI.

CI command:

TGE1> switch isolation enable

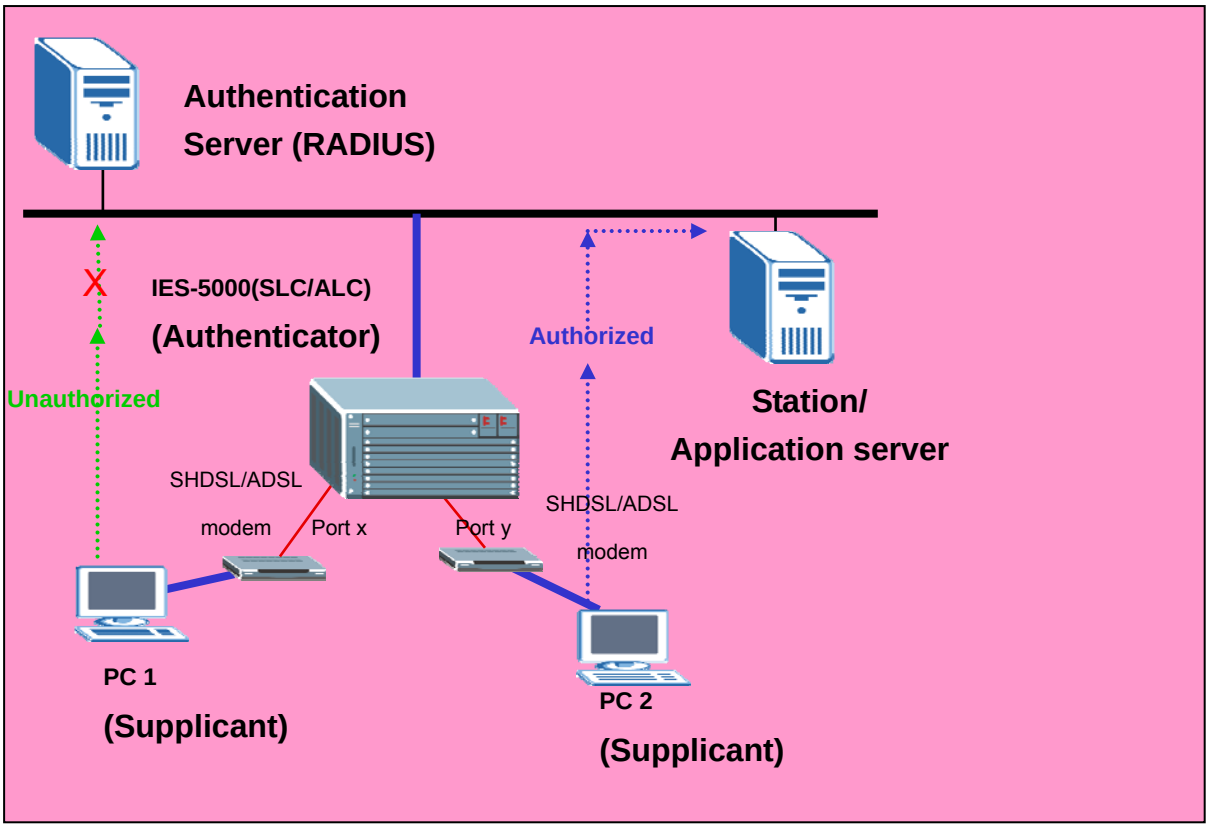
2. Prestige 660R-61(P791) Settings

Please refer to the steps in the previous application.

802.1x Application

IEEE 802.1x port-based authentication can be used to prevent unauthorized ports (clients) from gaining access to the network. It is an extended authentication protocol that allows support of RADIUS (Remote Authentication Dial in User Service, RFC2138, 2139) for centralized user profile management on a network RADIUS server.

The following figure shows a network example where the IES-5000 acts as an authenticator to provide 802.1x authentication. In this example, the supplicants (PC1 and PC2) want to gain access to the application server.



Setting up 802.1x

To set up an 802.1x infrastructure, we need to configure the authenticator, RADIUS and supplicants. In this example, we will use Microsoft 802.1x client as the supplicant and ZyXEL Vantage 50 as the RADIUS server. The following sections describe the procedures.

1. Authenticator Setup: IES-5000

1.1 RADIUS settings:

Enable 802.1x Authentication and specify the RADIUS server IP address, UDP port and shared Secret on the IES-5000. Make sure you enter the same UDP port and shared secret as the RADIUS server. Then save the settings to make them take effect.

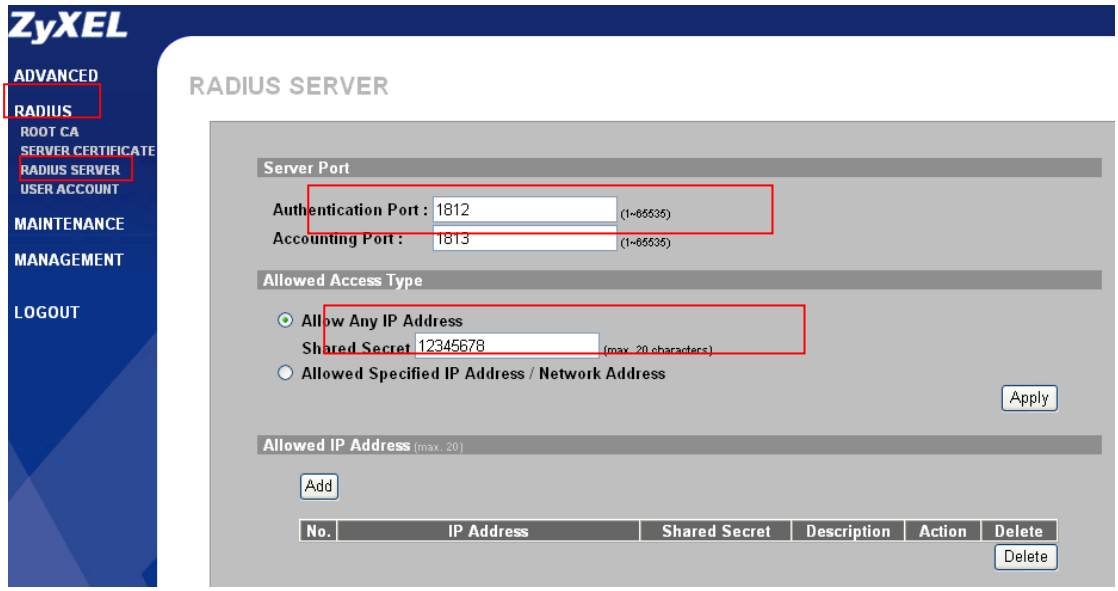
TGE1> sys sw dot1x enable
TGE1> sys sw dot1x set radius server 192.168.1.3
TGE1> sys sw dot1x set radius port 1812
TGE1> sys sw dot1x set radius sec 12345678
TGE1> config save

2. RADIUS Setup: Vantage 50

You can use any RADIUS server (such as Funk Steel-Belted RADIUS, Cisco Access Control Server or MeetingHouse Aegis server). In this example, we will use ZyXEL Vantage 50 as the RADIUS server. You can configure Vantage 50 through its web configurator (the default management IP address is 192.168.1.3).

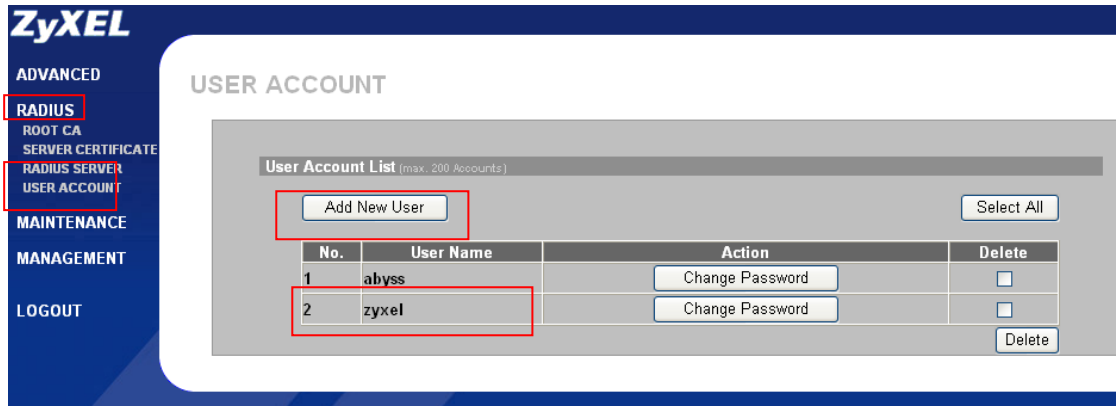
2.1 RADIUS server setup

Click **RADIUS** and **RADIUS SERVER** in the navigation panel to display the configuration screen as shown. You can use the default values or change the **Authentication port**, **Shared Secret** settings. Make sure these values MUST are the same as on the client.



2.2 Create a User Account

Click **RADIUS** and **USER ACCOUNT** in the navigation panel to display the configuration screen as shown. You can use existing user accounts or create a new one by clicking the **Add New User** button. Clients must enter the correct user name and password to log into the network.

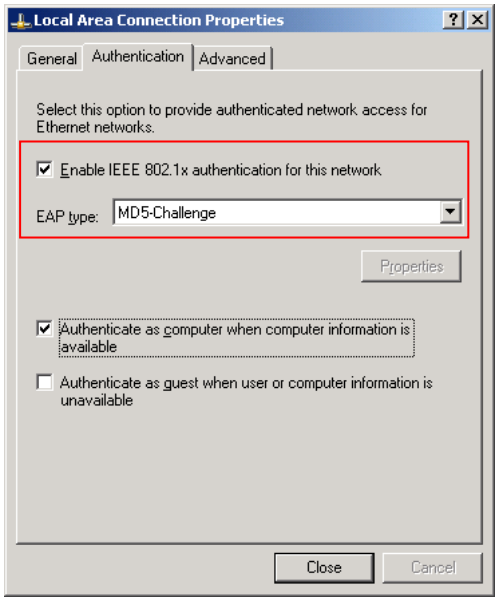


3. Supplicant Setup: Windows XP

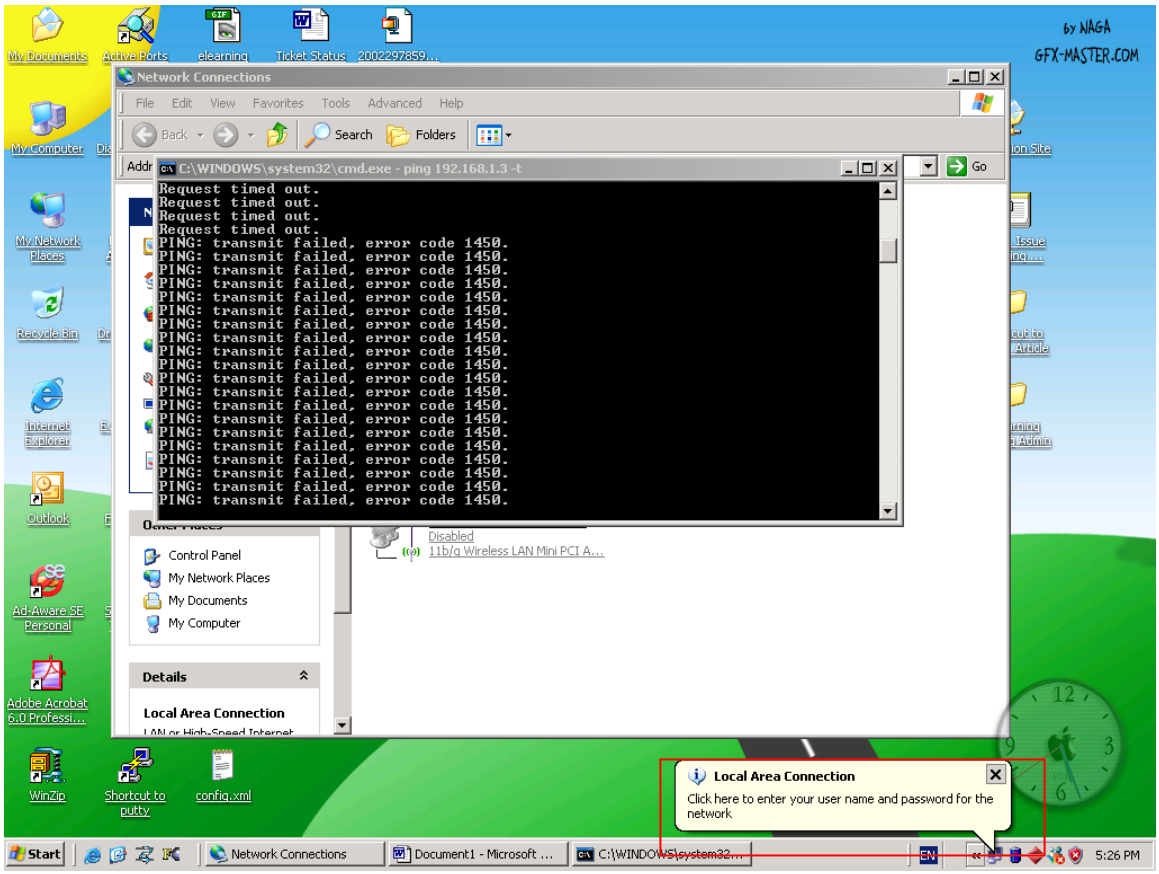
You can use any supplicant/client software (such as MeetingHouse Aegis client, Funk Odyssey client and Microsoft 802.1x client). In this example, we will use take Microsoft 802.1x client software.

3.1 802.1x/MD5-challenge setup

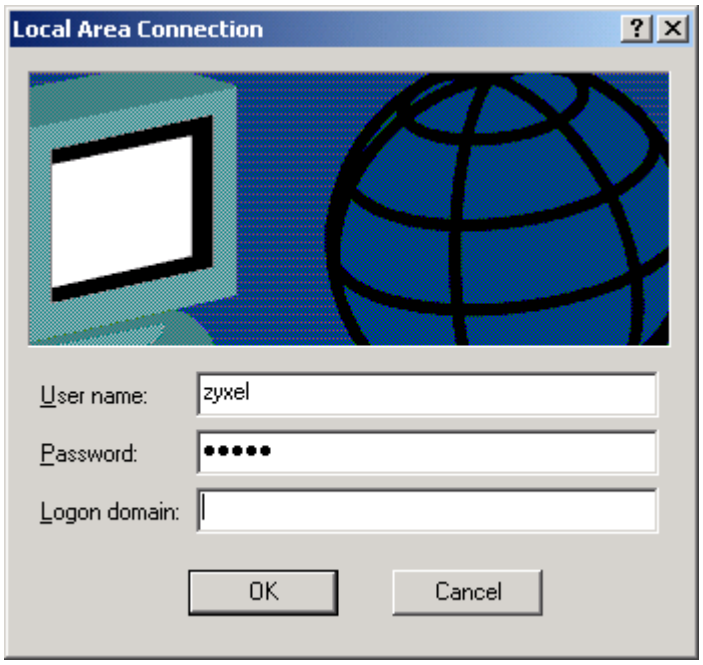
Open the **Local Area connection Properties** screen and click the **Authentication** tab. Select **Enable IEEE 802.1x authentication for this network** and select **MD5-challenge** in the **EAP type** field.



When the 802.1x authentication process starts, a message displays in the system tray prompting you to enter the account user name and password. The following figure shows an example.



Click on the message balloon to display the login screen where you can enter your account user name and password. After entering the required information, click **OK** to continue. Once the authentication process is successful, client setup is complete.



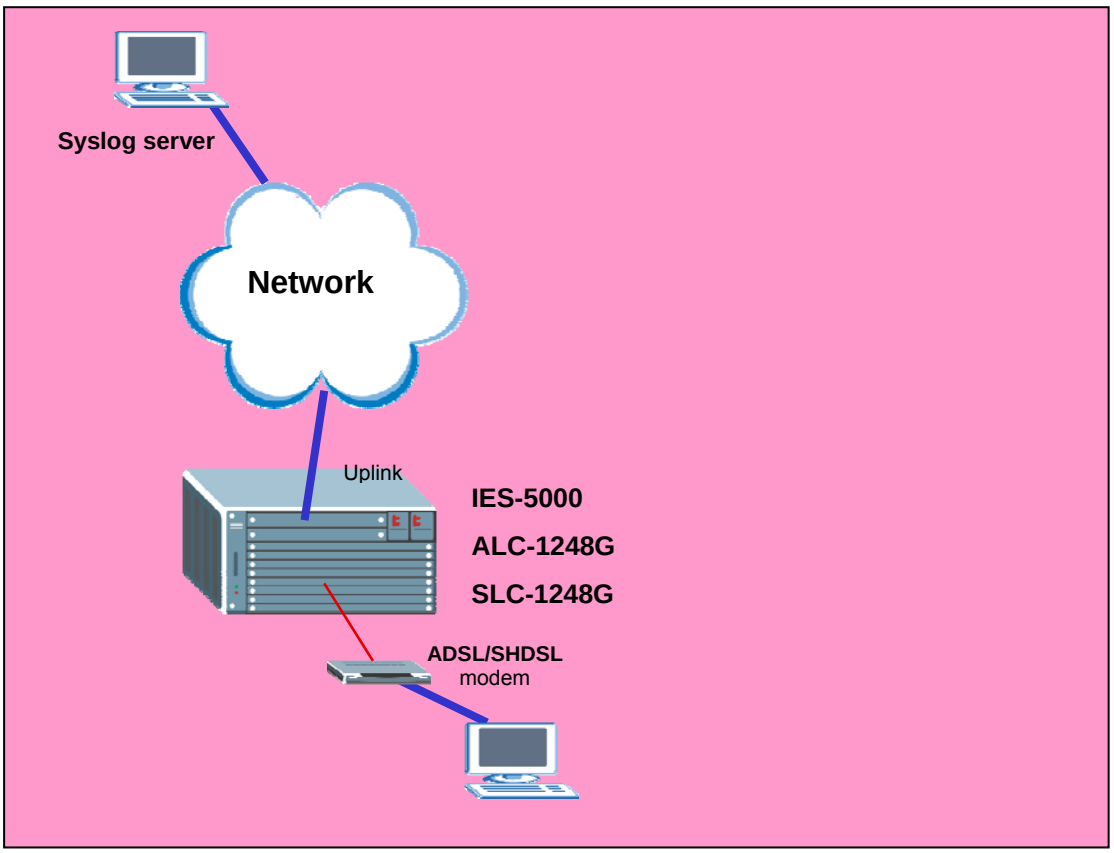
Once you are authenticated successfully, you can access the network. Otherwise, network access is not allowed through the DSL port on the CPE.

4. Prestige 660R-61 Settings

Please refer to the procedures described in the previous application.

Syslog Server Application

You can set your ZyXEL product to send system logs to an external syslog server (such as Syslodd in Unix and Kiwi Syslog Daemon (http://www.kiwisyslog.com/)). When the DSL or Ethernet connections are up or down, the IES-5000 sends a log record to the syslog server. You must install the syslog server on the network that the IES-5000 can access. The following figure shows an example.

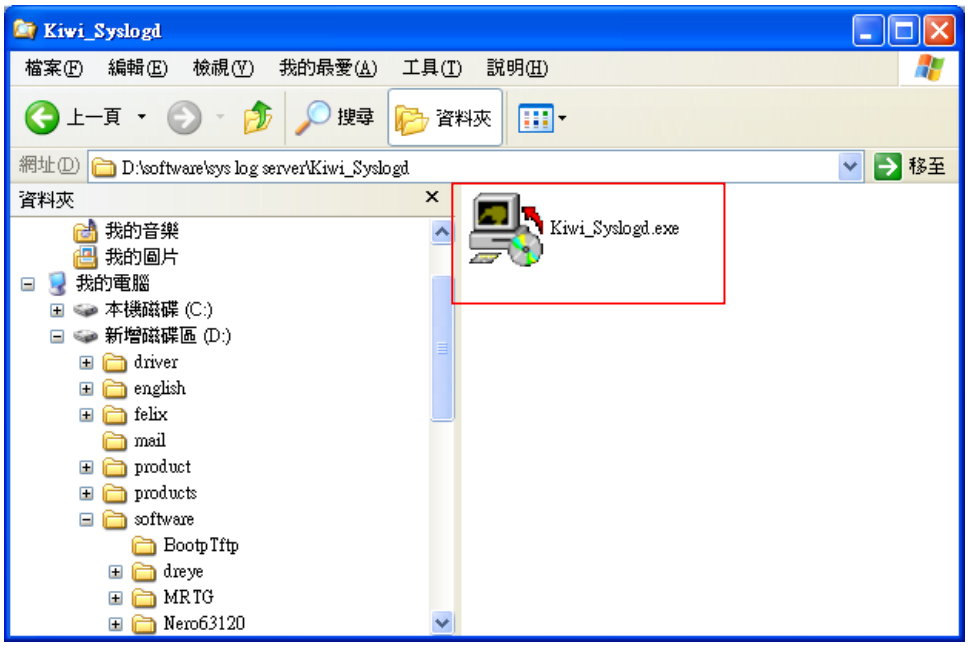


Setting up a Syslog server

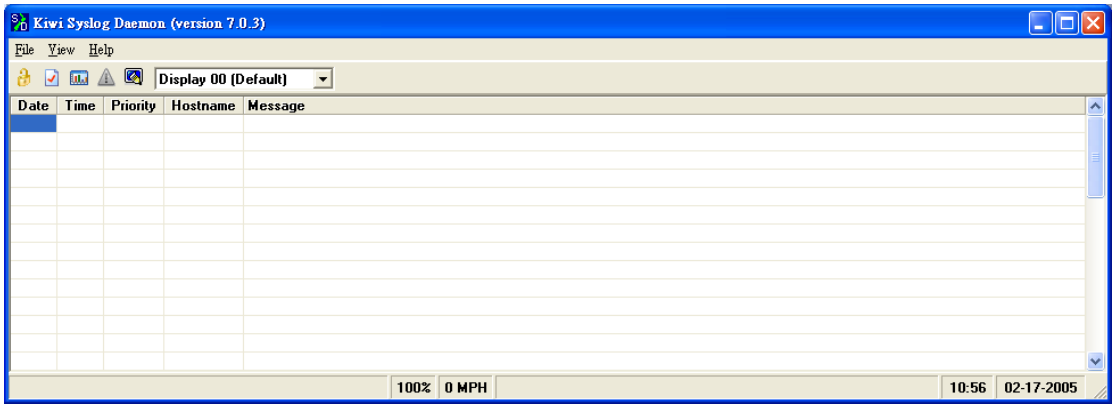
In this section, we will show you how to configure the IES-5000 and Kiwi Syslog server. The subsequent sections describe the detailed configuration steps.

1. Installing and Running Kiwi's Syslog Server

Download the Kiwi syslog daemon installation file from the web site and double-click the file to start the installation process. Follow the on-screen description to install.



After the installation process is complete, start the daemon from the **Start** menu. A screen displays as shown. In this example, assume that the syslog server's IP address is 192.168.1.77.



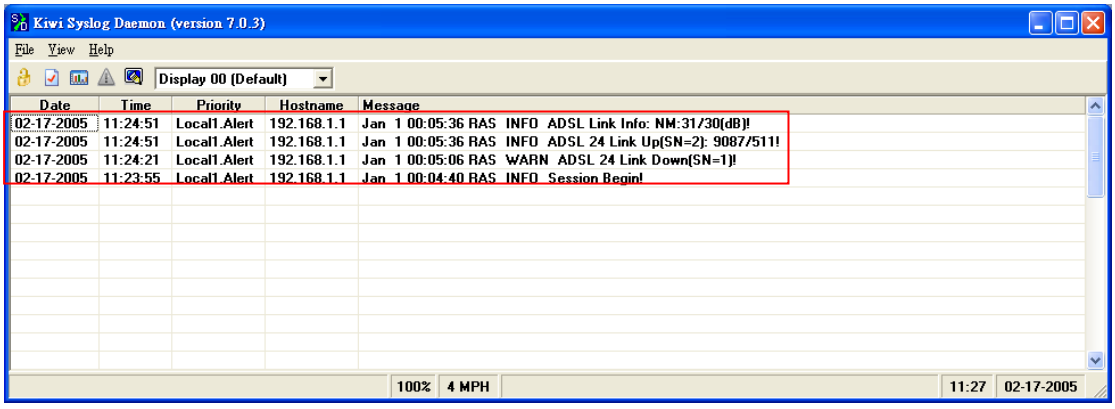
2. IES-5000 settings

On the IES-5000, enable syslog logging and specify the IP address of the syslog server (192.168.1.77 in this example). Specify where (Local 1 through Local 7) you want to store the logs and then save the settings.

CI command:

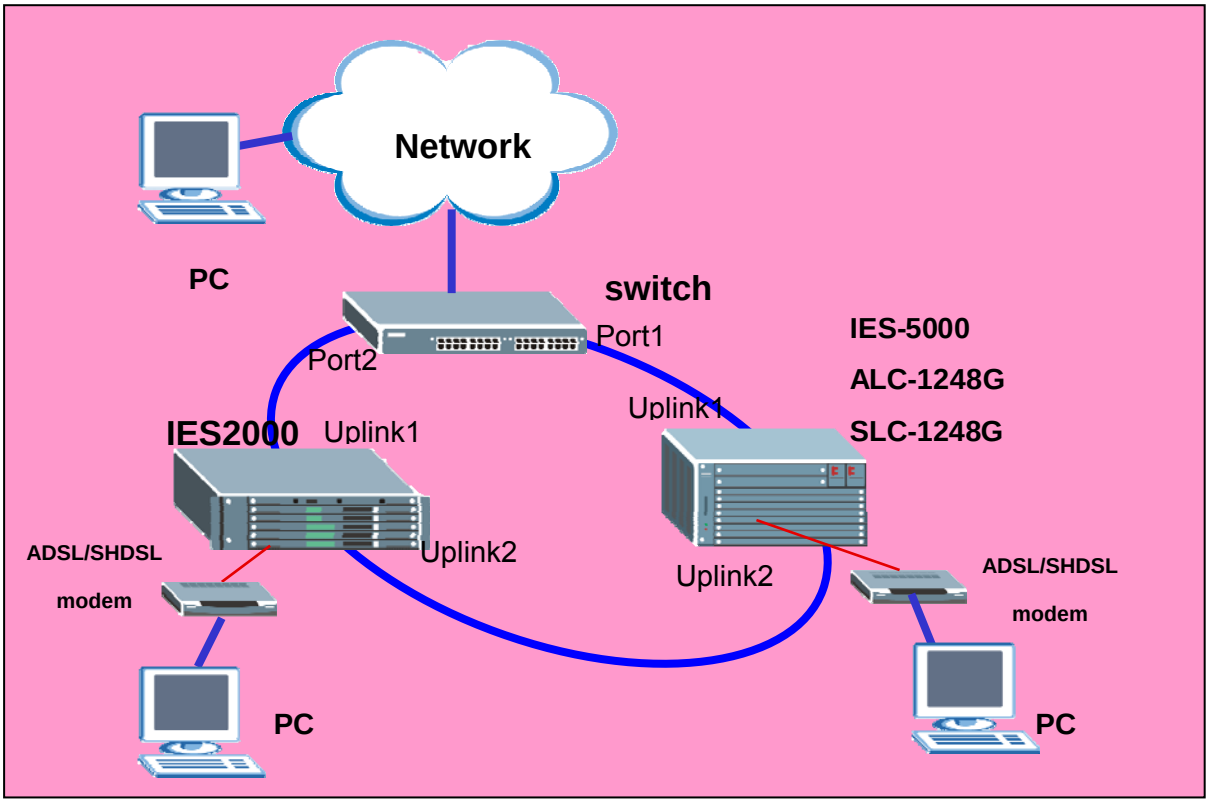
TGE1> sys syslog enable
TGE1> sys syslog server 192.168.1.77
TGE1> sys syslog facility 1
TGE1> config save

When the DSL connection is up or down, the IES-5000 sends a log record to the syslog server. You can see the new entry in the syslog server. The following shows an example.



Ring Topology Application

A ring topology provides network redundancy. This means that when a link is down, the entire network can still be up as traffic is forwarded through another route or gateway. However, to prevent network loops in a ring topology, you must enable RSTP/STP on the network. The following figure shows a ring network example.



Setting up a Ring Environment

This section shows you how to set up a ring network using an IES-5000, IES-2000 and an ES-4024 switch. The computers should be able to connect to each other even though an uplink connection is down. The following sections describes the configuration steps in detail.

1. IES-5000 settings

1.1 Activating Spanning Tree protocol on Ethernet Ports

Before you set up the ring topology, enable spanning tree protocol on the Ethernet

ports 1 and 2. The following shows the CLI commands.

CI command:

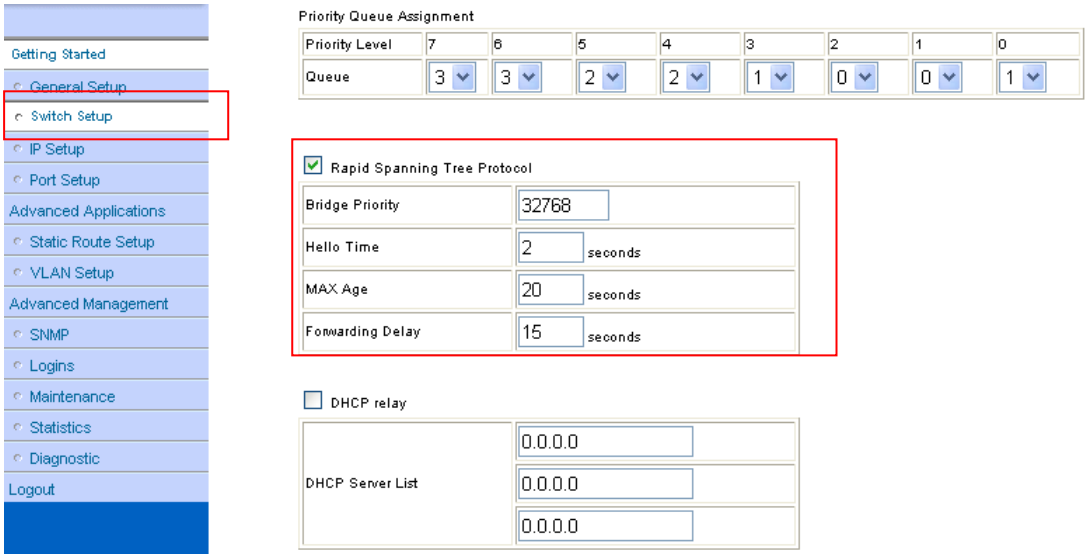
TGE1> sys sw rstp enable
TGE1> sys sw rstp port enable 1
TGE1> sys sw rstp port enable 2

2. Setup IES-2000

2.1 Activating Spanning Tree protocol

This section shows how to enable STP on the IES-2000 using the web configurator.

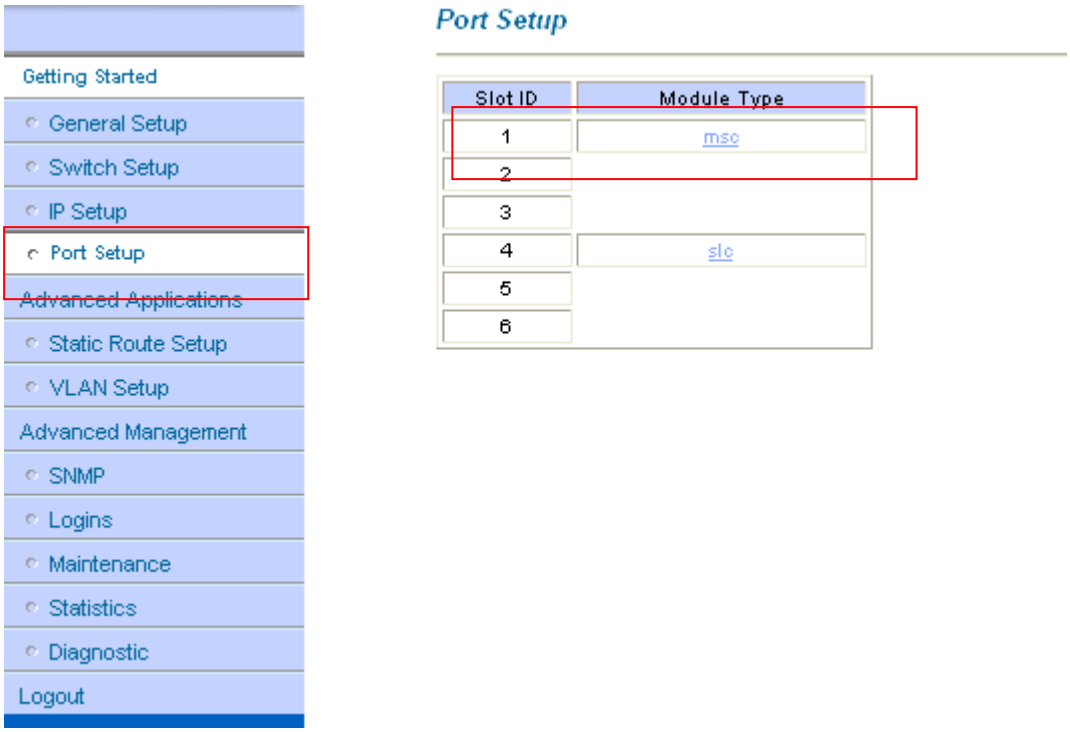
Access the web configurator and click **Switch Setup** in the navigation panel to display the configuration screen as shown. Then select the **Rapid Spanning Tree Protocol** option to enable it.



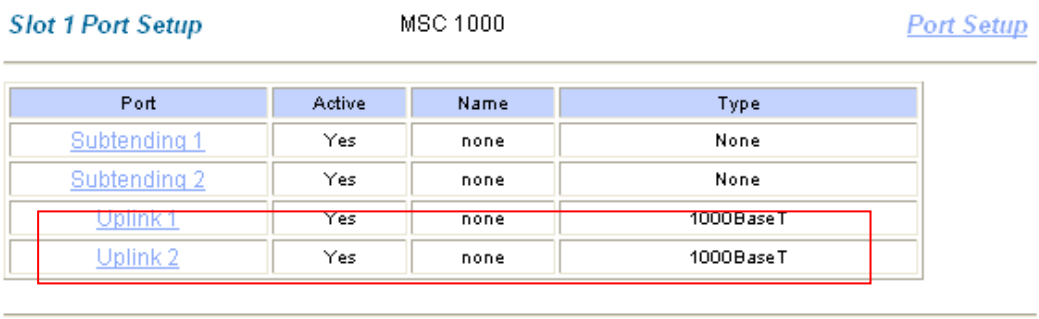
2.2 Activating Spanning Tree protocol on Ethernet ports

After you have activated STP on the system, you must activate STP on the Ethernet ports.

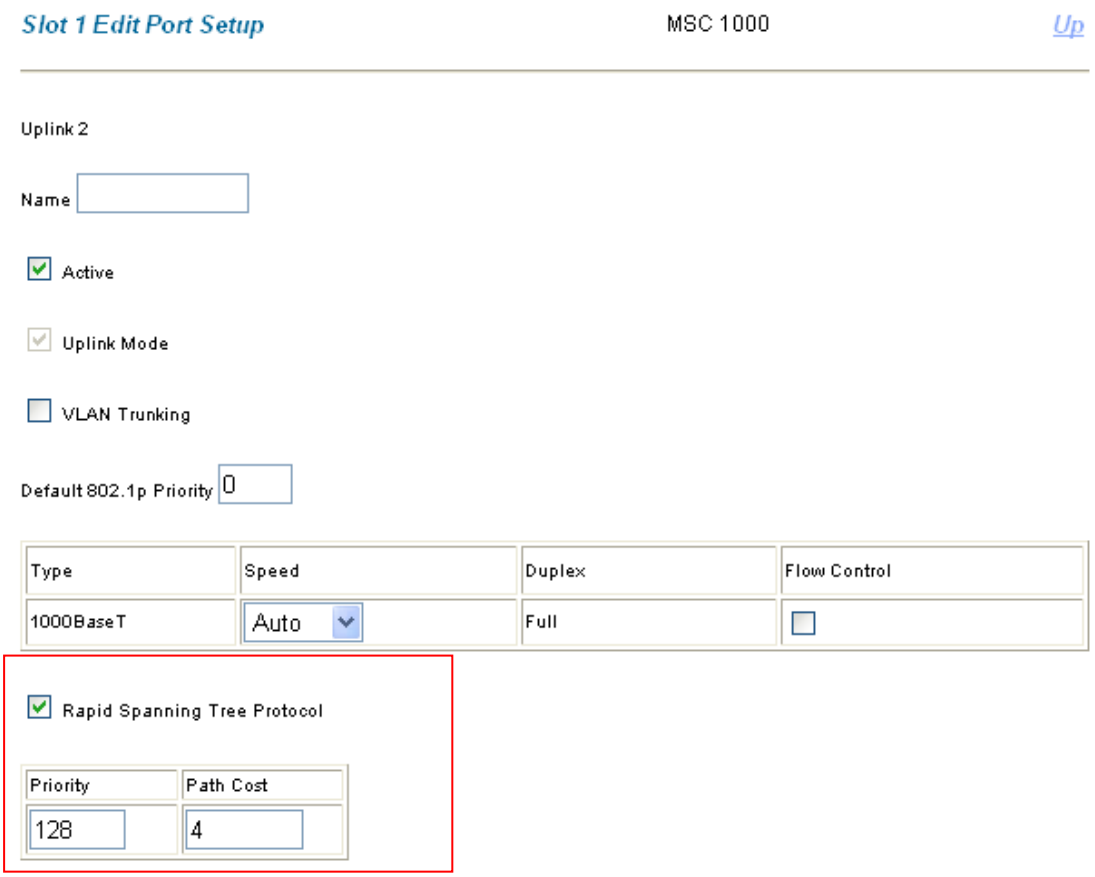
In the web configurator, click **Port Setup** in the navigation panel to display the configuration screen as shown. Click **msc** to display the configuration screen for the Ethernet ports on the MSC line card.



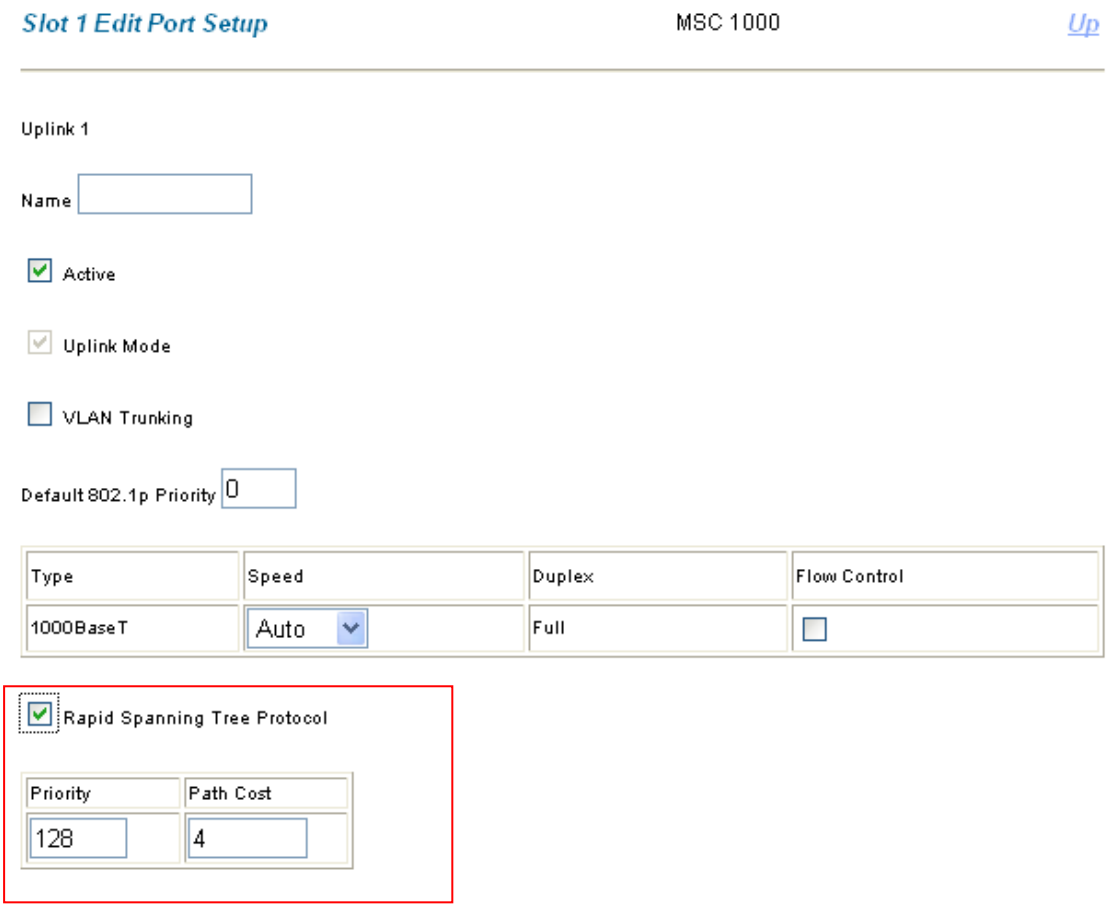
Click **Uplink2** to configure this port.



Select **Rapid Spanning Tree Protocol** to enable it on the port.



Follow the same procedure to activate STP on uplink port 1. The following figure shows an example.

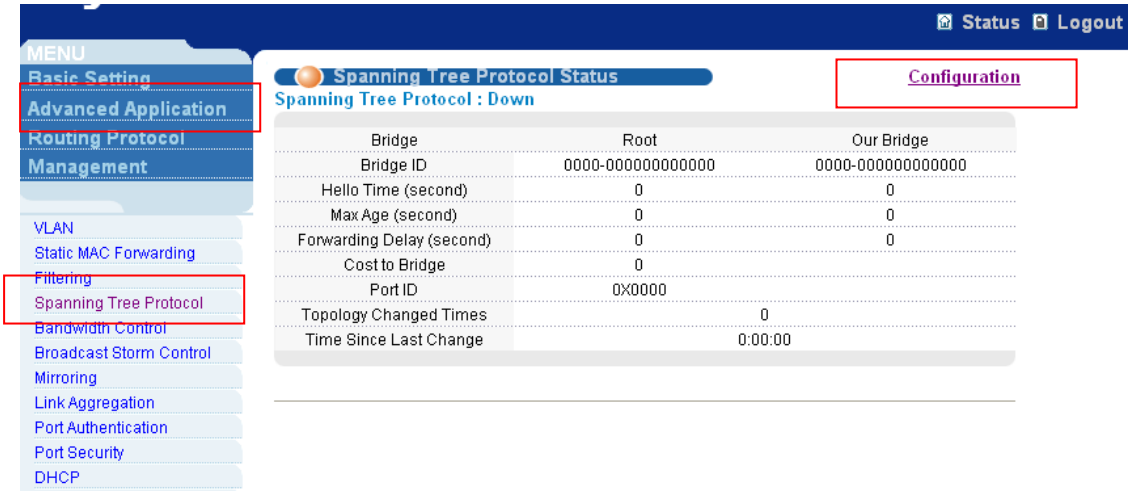


3. ES-4024 Settings

3.1 Activating Spanning Tree protocol

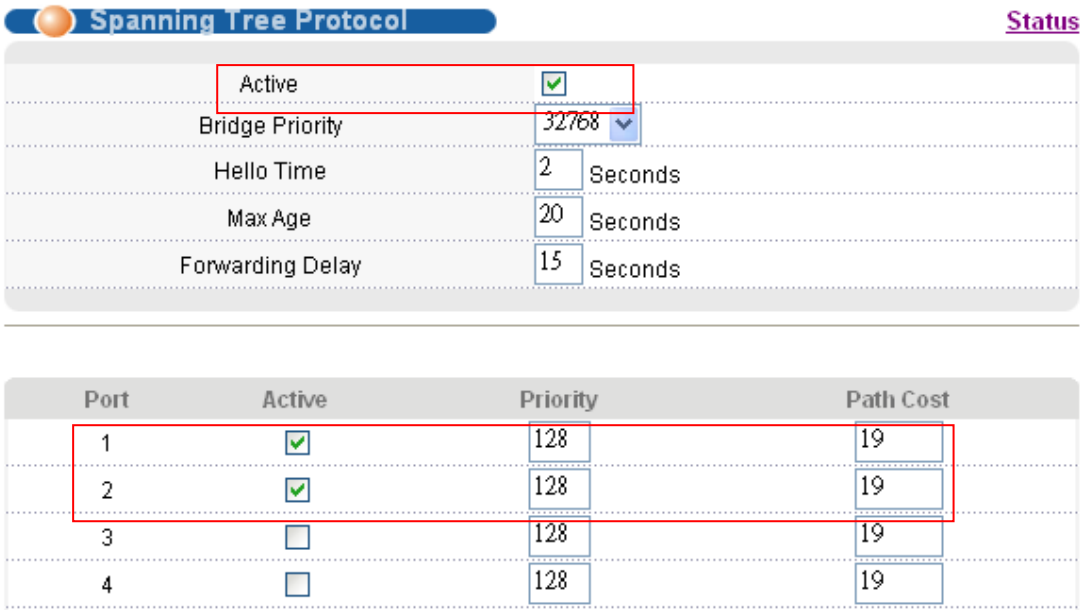
This section shows you how to enable STP on the switch.

Log into the web configurator on the ES-4024 and click **Advanced Application** > **Spanning Tree Protocol** in the navigation panel. The main **Spanning Tree Protocol Status** screen displays. Click **Configuration** to configure spanning tree protocol settings.



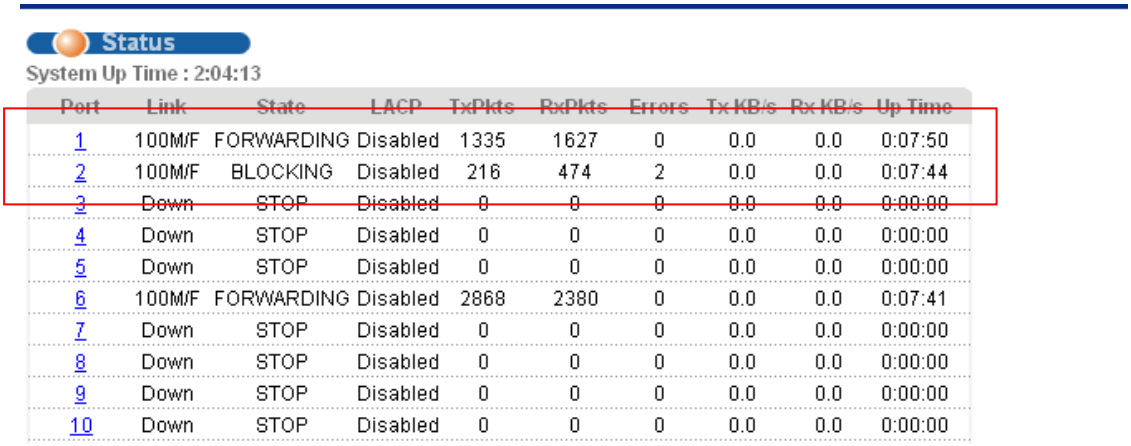
Select **Active** to enable Spanning Tree Protocol on the system and then enable STP on

ports 1 and 2.



4. Status Results

After you connect the uplink port 1 on IES-2000 to port 2 on the ES-4024, the state of port 2 becomes **BLOCKING**.



To test the RSTP/STP mechanism, disconnect the Ethernet cable between uplink port 1 on the IES-5000 and port 1 on the ES-4024. The computers can still access the network through the CPE devices since traffic now goes through IES-2000.
Check the state of port 2 on the ES-4024. It has become **FORWARDING**.

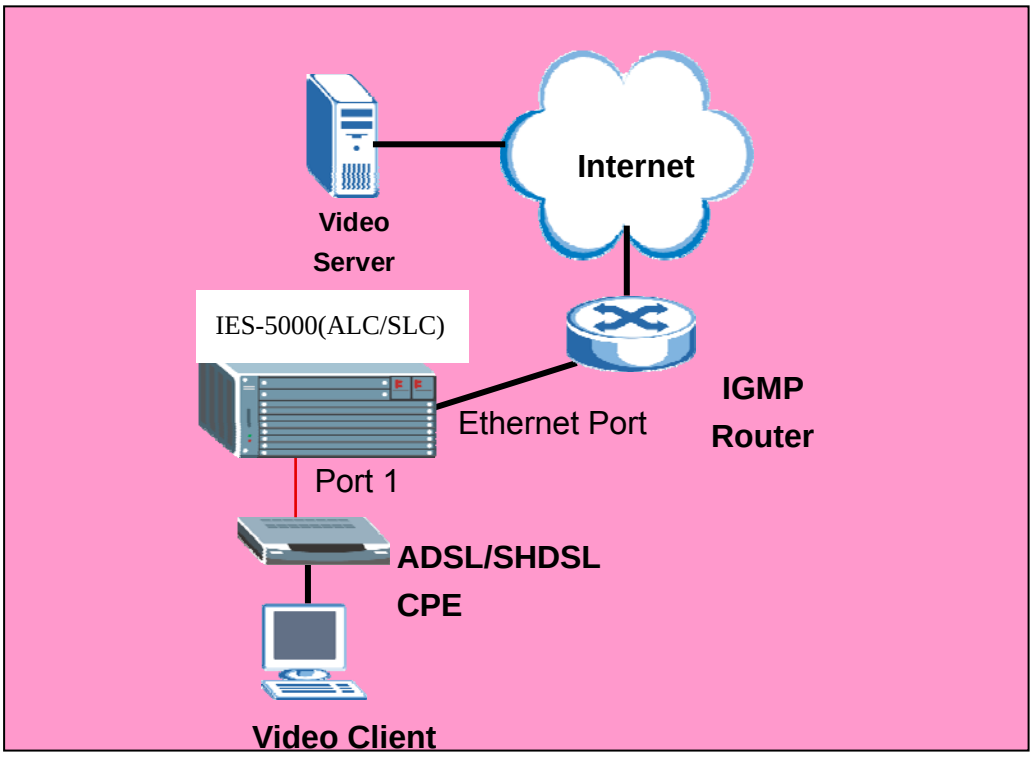
Status

System Up Time : 2:11:04

Port	Link	State	LACP	TxPkts	RxPkts	Errors	Tx KB/s	Rx KB/s	Up Time
1	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
2	100M/F	FORWARDING	Disabled	217	683	2	0.0	0.0	0:01:44
3	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
4	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
5	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
6	100M/F	FORWARDING	Disabled	3278	2698	0	0.0	0.0	0:14:32
7	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00

IGMP Snooping/IGMP Filtering Application

Without IGMP snooping, multicast traffic is treated in the same manner as broadcast traffic, that is, it is forwarded to all ports. With IGMP snooping, multicast traffic of a group is only forwarded to ports that have members of that group. IGMP snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through the IP-DSLAM. IGMP filtering allows a port to join specific IGMP groups. This feature is useful for video service providers as they only need to allow certain, but not all, channels (or multicast groups) on specific ports.



Setting up IGMP snooping/IGMP filtering

In this section, we will show you how to configure IGMP snooping and filtering on the IES-5000. For details on configuring a video server and the corresponding subscriber device, refer to the documentation that comes with the devices.

For this application example, the video server provides three channels:

- movie 1 in the 240.10.10.8 multicast group
- movie 2 in the 240.10.10.9 multicast group
- movie 3 in the 240.10.10.10 multicast group

If IGMP snooping is not enabled or if IGMP filtering is not enabled on the ports, all subscribers can watch movies from each channel. We want to limit a subscriber to view movies from movie channels 1 and 2 only.

1. IES-5000 settings

1.1 Activating IGMP Snooping

Enable IGMP Snooping on the IES-5000.

CI command:

TGE1> multicast igmp enable snooping

1.2 Setting up IGMP Filtering

Next enable IGMP filtering and configure IGMP filtering profiles for a subscriber to limit the movie channels the subscriber can watch.

For this example, we want to allow the subscriber to join the movie 1 and movie 2 groups. This means that traffic from the 240.10.10.8 and 240.10.10.9 multicast groups are sent to the port to which the subscriber is connected.

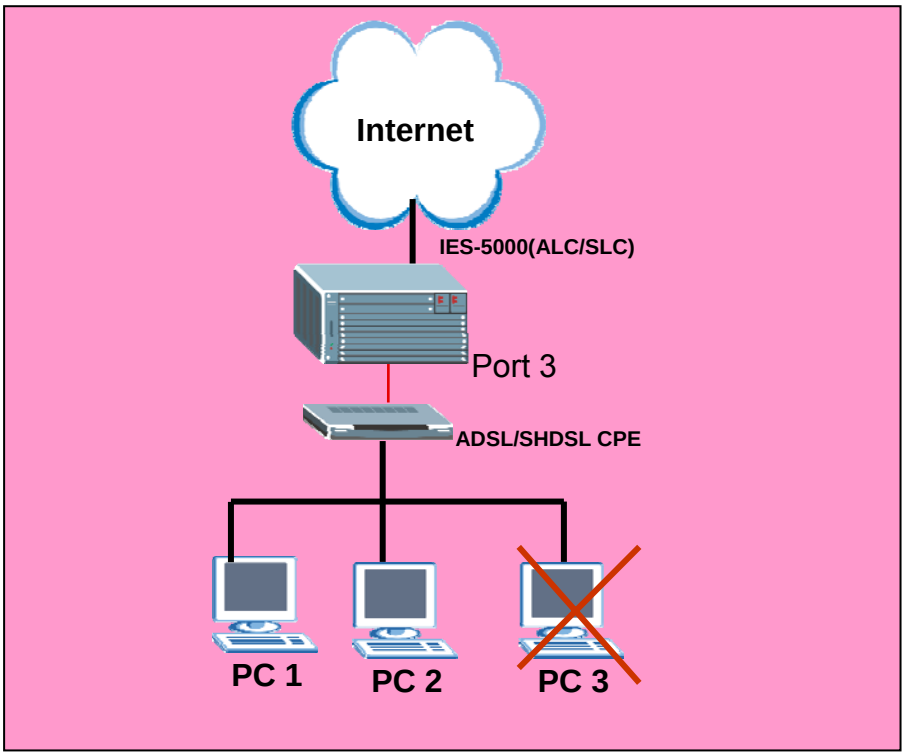
On the IES-5000, create an IGMP filter profile (Subscriber1) and apply the profile to port 1. Then apply the profile to the subscriber port (7-1). Save the settings to make it take effect.

CI command:

TGE1> profile igmpfilter set Subscriber1 1 224.10.10.8 224.10.10.9
TGE1> multicast igmpfilter set 7-1 Subscriber1
TGE1> config save

Limiting Internet access to users on specific DSL ports

Some ISPs may want to limit the number of computers behind certain DSL ports to access the Internet or allow computers with specific MAC addresses to access the Internet. These tasks can be easily done with the port security and MAC address filtering features on the IES-5000.



Setting up MAC Filter/Port Security

In this section, we will show you how to configure the IES-5000 to allow only computers with the specified MAC addresses to access the Internet through port 3.

1. IES-5000 settings

1.1 Configuring MAC filter

On the IES-5000, enable MAC filtering on port 3 and specify the MAC addresses allowed. This sets the IES-5000 to allow only computers with the specified MAC addresses on port 3 to access the Internet. A computer with any other MAC addresses

will not be able to access the Internet on port 3. Save the settings to make the changes take effect.

CI command:

```
TGE1> lcman port macfilter enable 7-3
TGE1> lcman port macfilter set 7-3 00:a0:c5:12:34:56
TGE1> lcman port macfilter set 7-3 00:a0:c5:77:88:99
TGE1> config save
```

1.2 Configuring Port Security

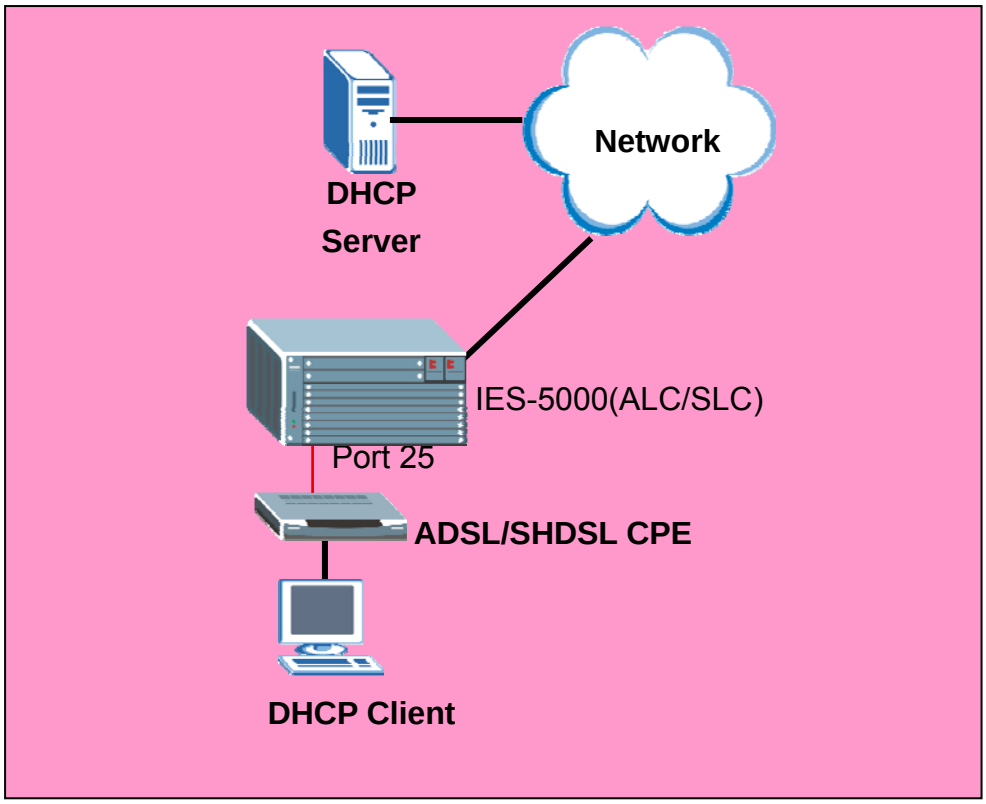
Alternatively, you can enable port security on port 3 in slot 7 and specify the number of MAC addresses allowed to access through the port at the same time. In this example, we will only allow one user to access at a time. That means when the user is logged in for Internet access on port 3, any user will be blocked.
Note that you cannot activate MAC filtering and port security at the same time.

CI command:

```
TGE1> lcman port maccount enable 7-3
TGE1> lcman port maccount set 7-3 1
TGE1> config save
```

DHCP Relay Option 82 Application

In some cases, ISPs may want to limit the number of IP addresses assigned to the users or assign certain IP addresses based on the DSL port, VLAN ID and option 82 string. To set up this flexible client IP address assignment scheme, configure the They DHCP Relay Option 82 feature and set up a DHCP server that supports the Option 82 function. The following figure shows a network example.



Setting up DHCP Relay Option 82

In this application example, we will show you how to configure the IES-5000 to assign a specific IP address in the client IP pool to a computer based on its DSL port, VLAN ID and the option 82 string.

For this example, assume that the computer is connected to DSL port 25 with an Option82 string of “5000” in VLAN 1. We will use the IP Commander DHCP server (192.168.1.99) to assign this computer an IP address in the client IP pool of 192.168.1.201~192.168.1.203.

1. IES-5000 settings

On the IES-5000, enable DHCP relay and specify the IP address of the DHCP server (192.168.1.99). Then enable Option82 and enter “5000” as the string.

CI command:

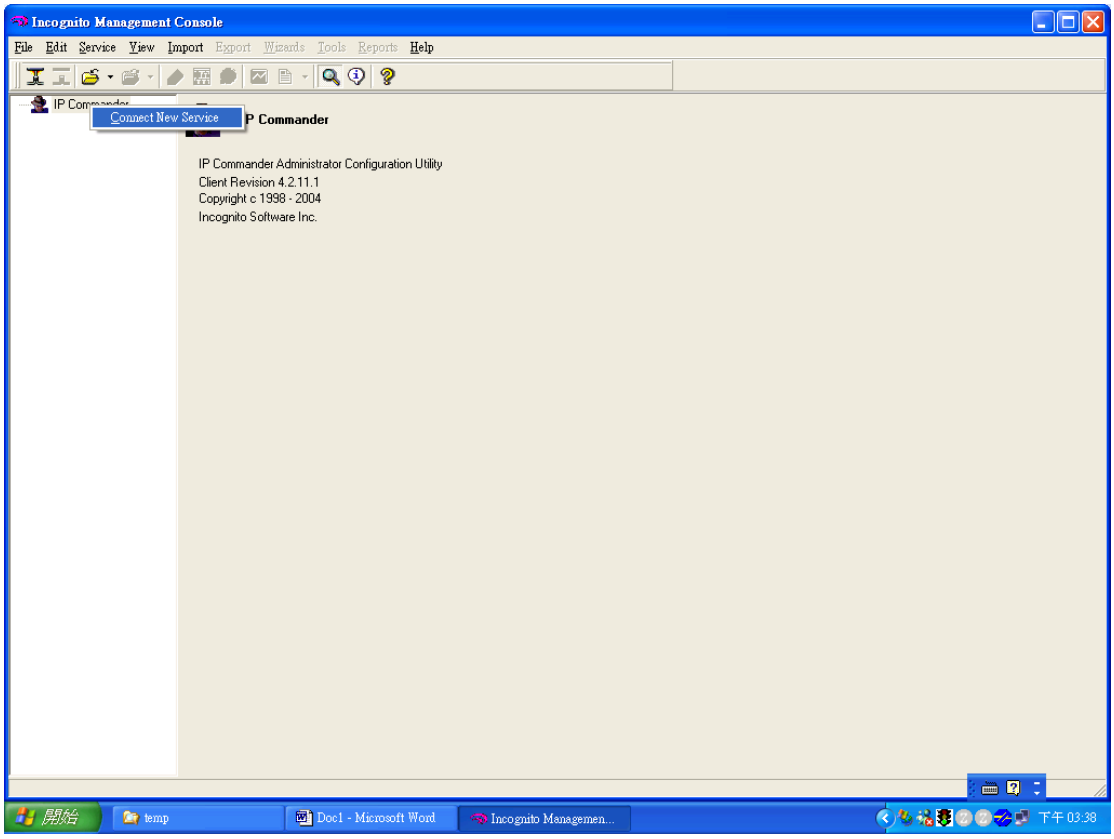
TGE1> ip dhcprelay enable
TGE1> ip dhcprelay relay enable
TGE1> ip dhcprelay server 1 192.168.1.99
TGE1> ip dhcprelay relayinfo add 5000

2. CPE settings

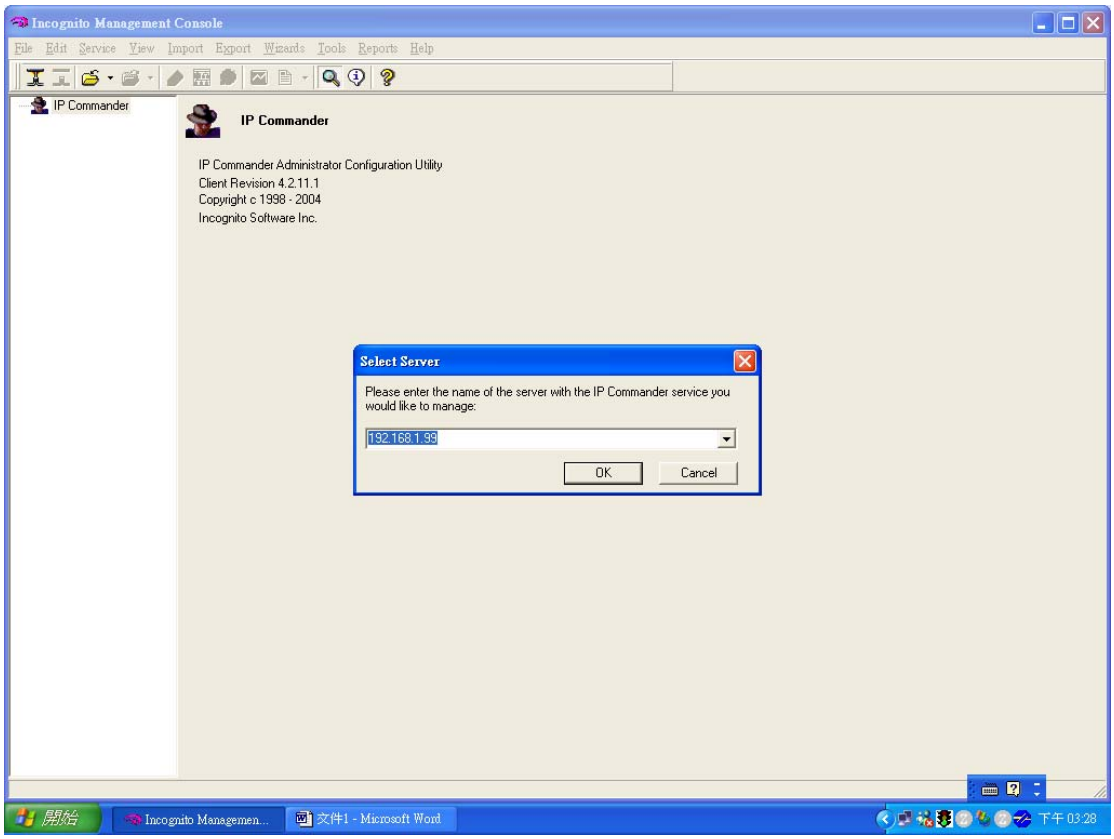
Connect a CPE device to DSL port 25. Refer to the previous sections on how to configure the CPE device.

3. IP Commander settings

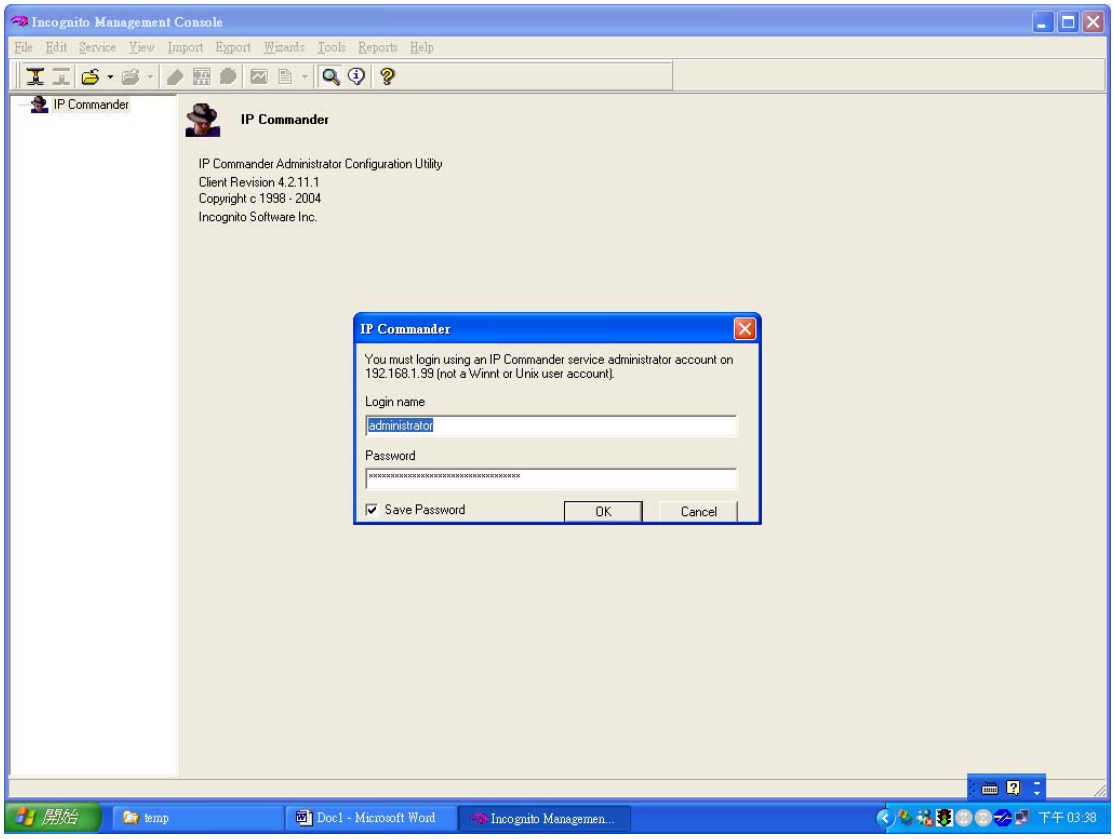
Display the IP Commander screen and right-click on **IP Commander** and then click **Connect New Server**".



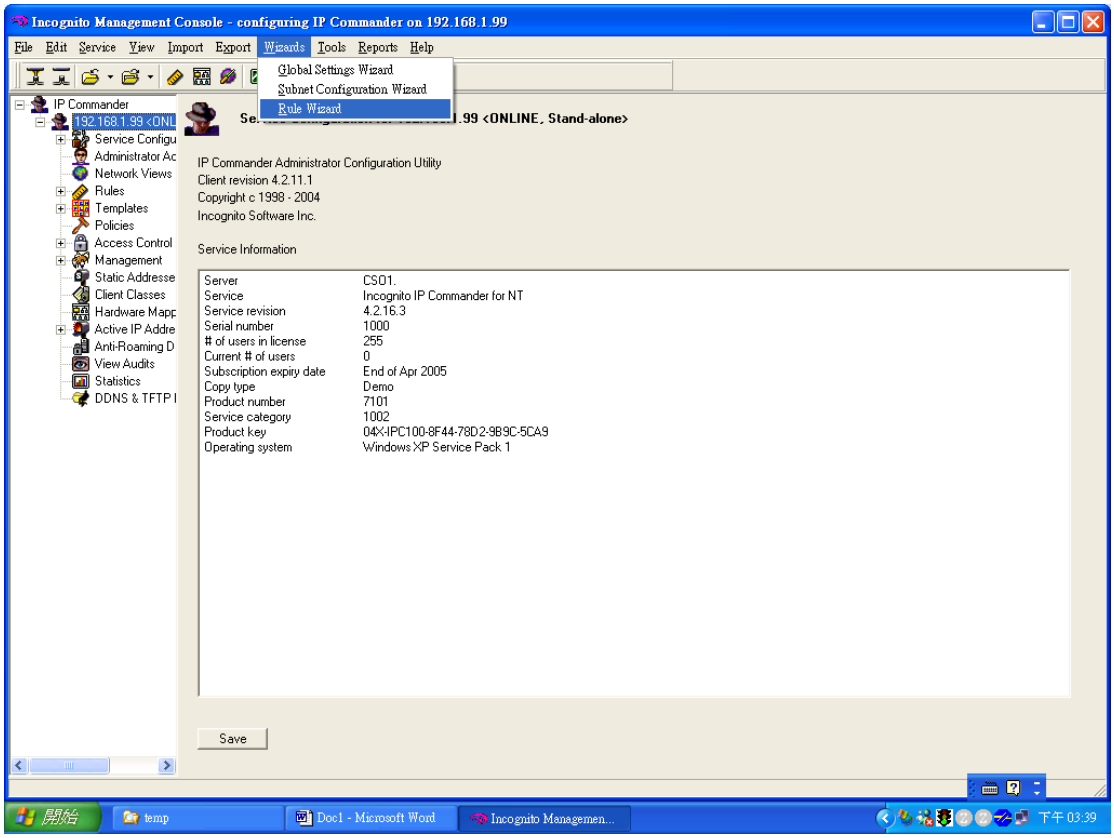
Enter the IP address (for example, 192.168.1.99) or domain name of the DHCP server and click OK.



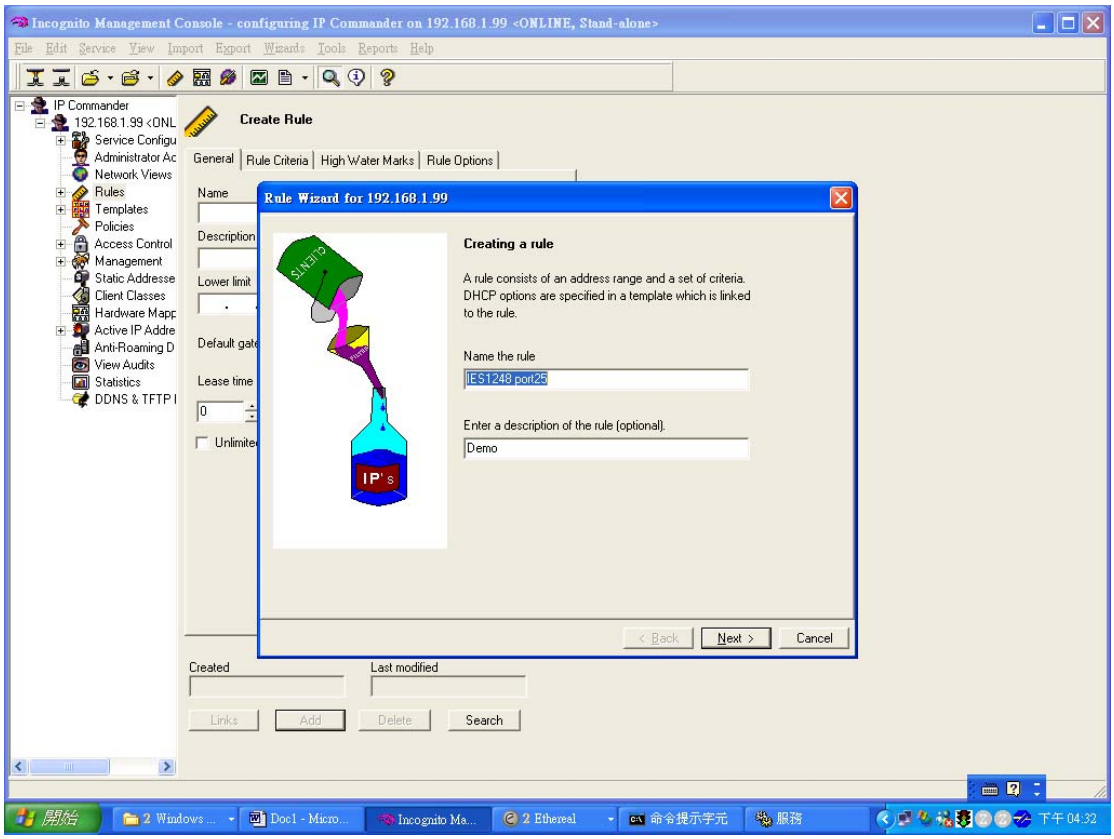
Enter the login user name and password. The default user name is “administrator” and the password is “incognito”.



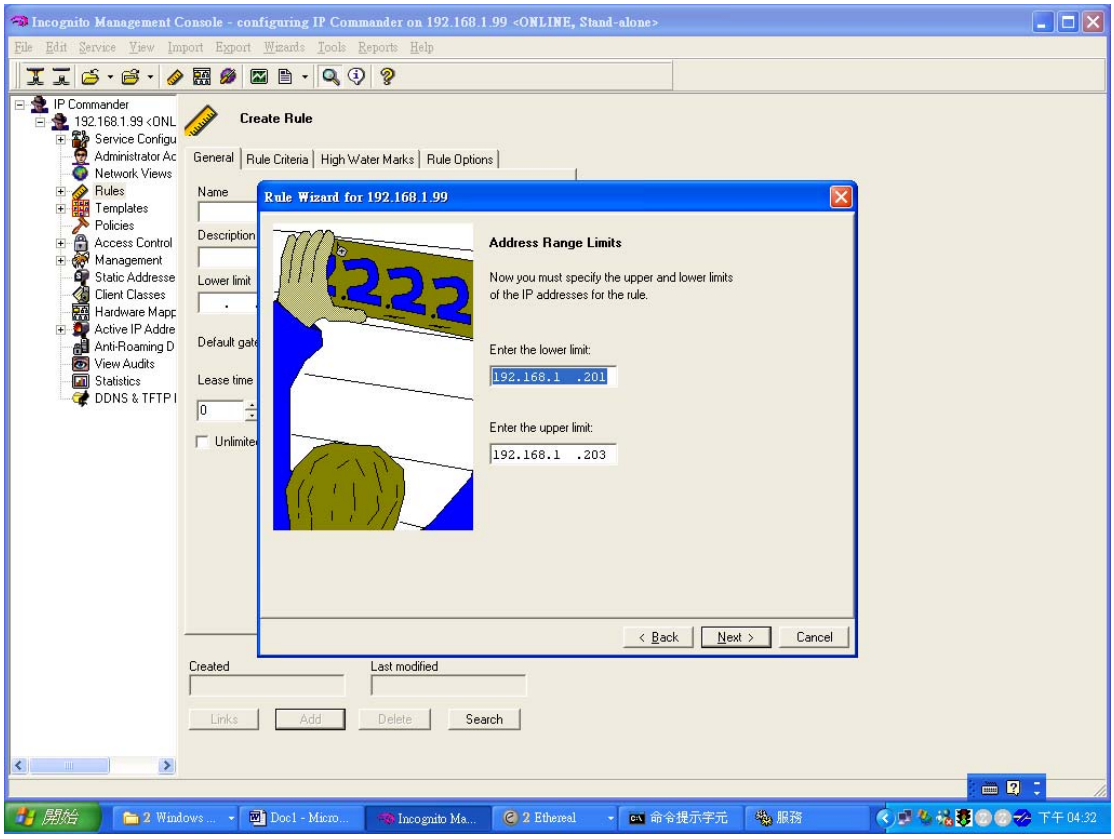
A screen displays as shown. Make sure that the status of your DHCP is **online**. Then click **Wizards** > **Rule Wizard** in the tool bar.



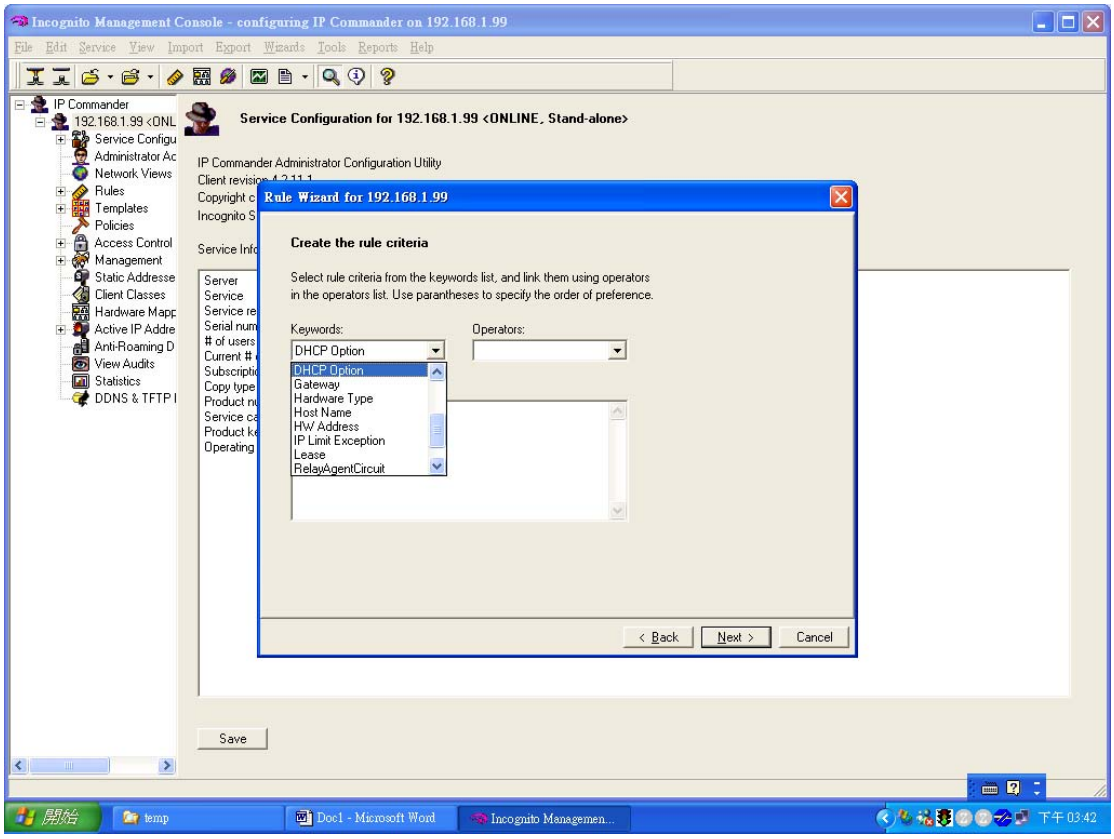
Enter a name and description for the new rule.



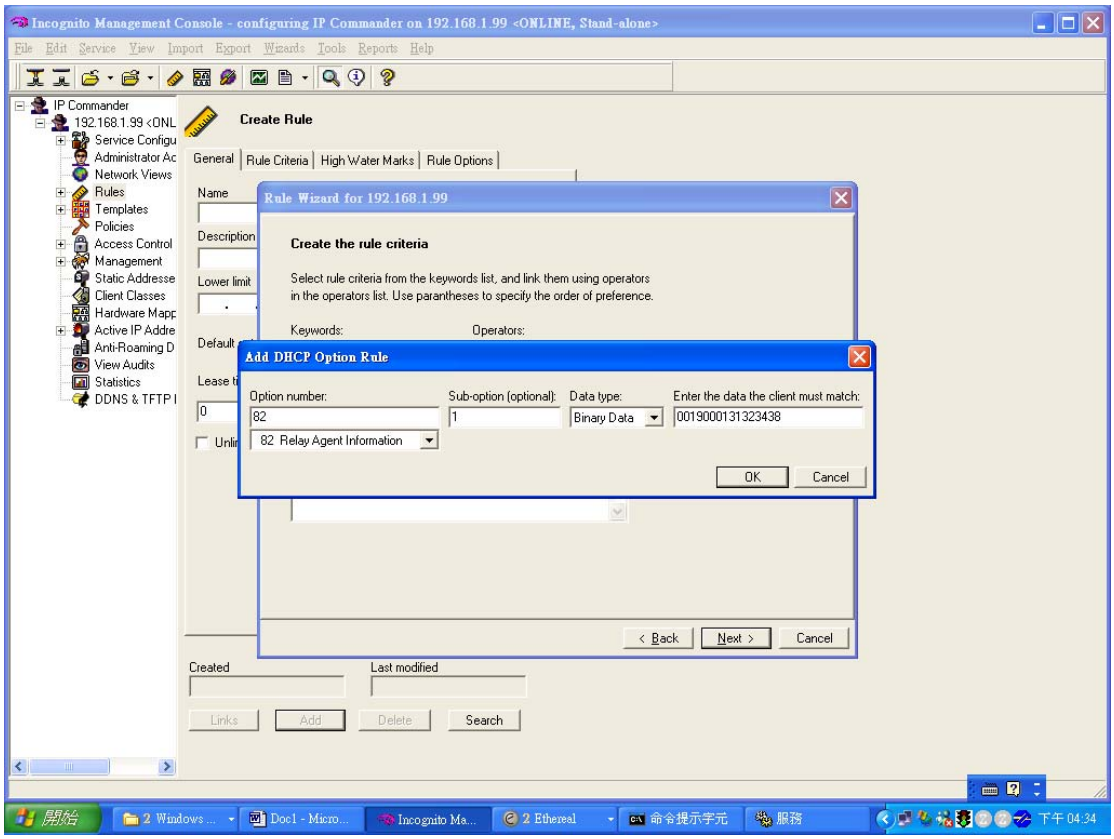
Assign one or a range of IP addresses for this rule. For this example, set the client IP pool in the 192.168.1.201 ~ 192.168.1.203 range.



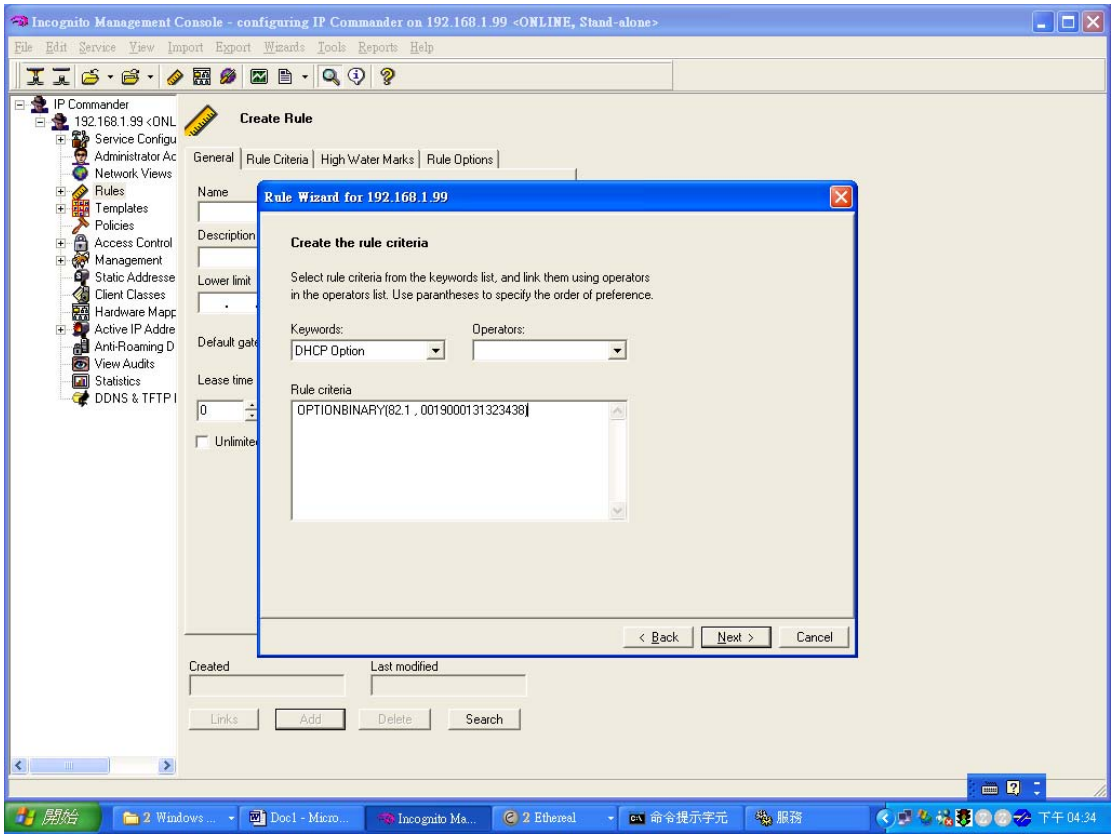
Select **DHCP Option** in the **Keywords** field.



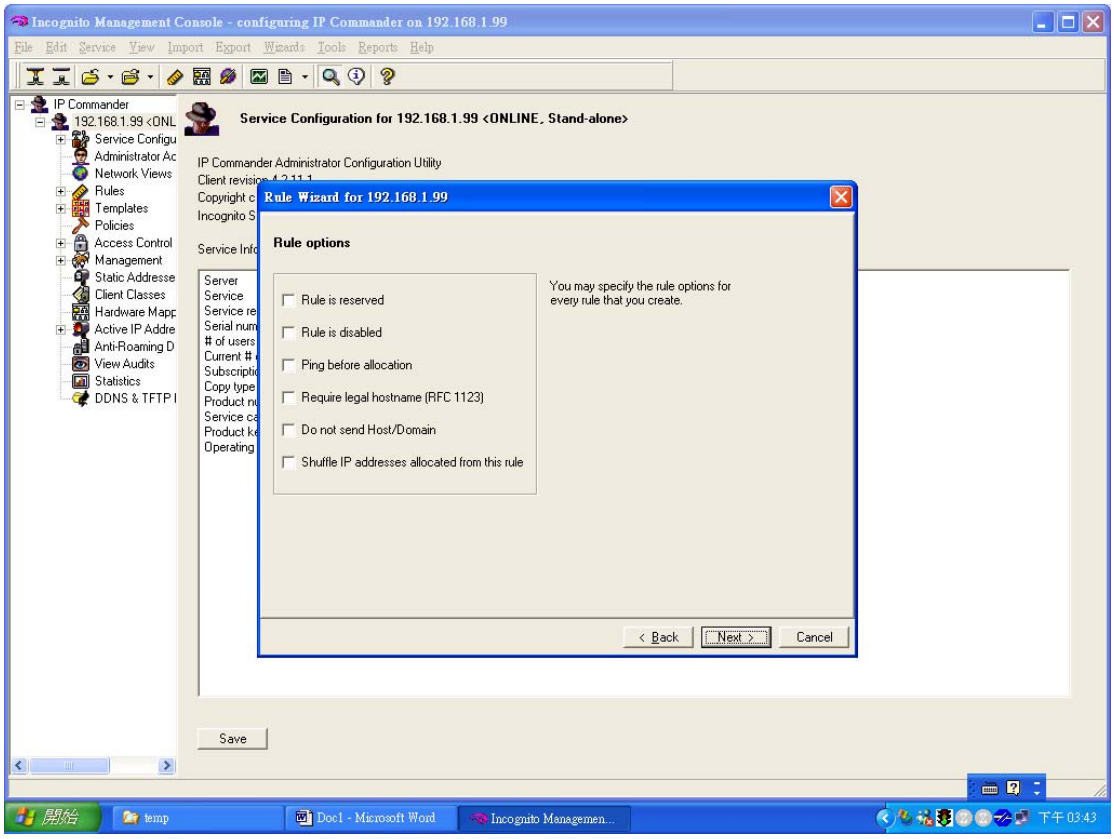
A configuration screen displays. Set the fields in the screen as shown.
Select 82 Relay Agent Information under the Option number field. Enter 1 in the Sub-option field and select the Binary data type.
For port 25, VLAN 1, option string “5000”, enter “0019000131323438” as the key value and click OK. Note that the first two bytes define the port number, the second two bytes define the VLAN ID and the subsequent bytes indicate the Option82 string.



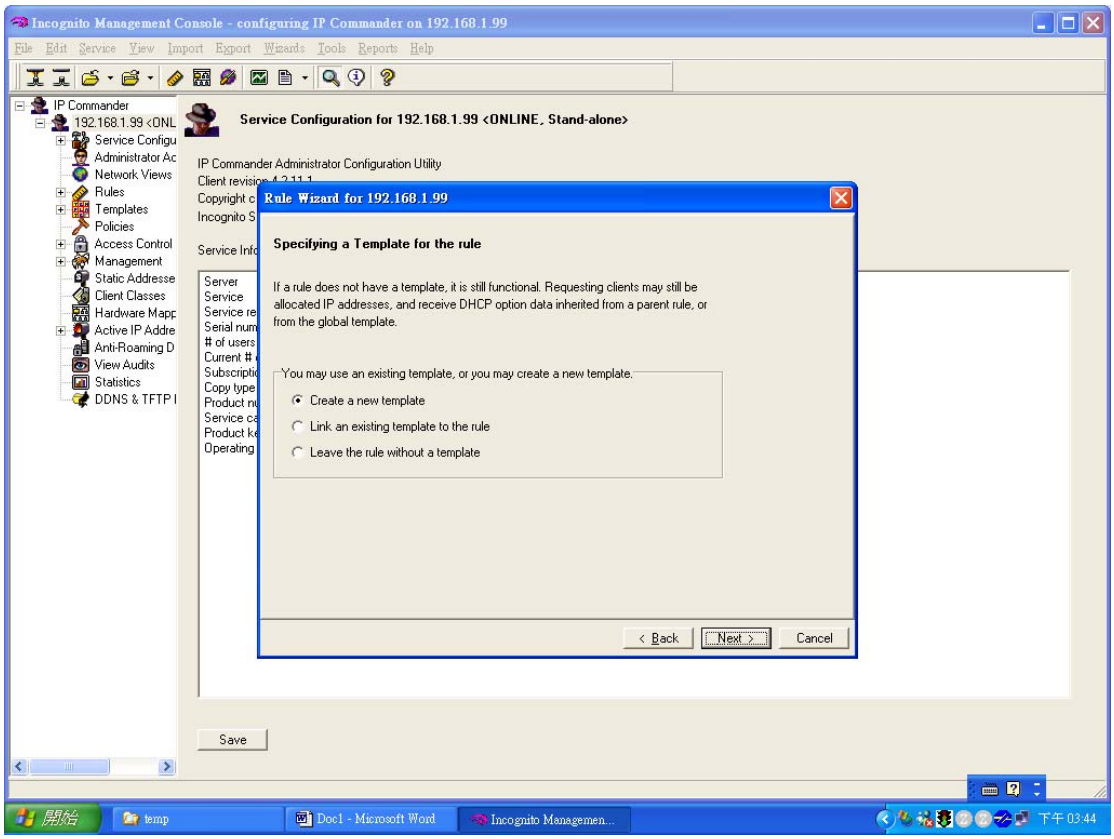
After you have finished the rule wizard settings, the following screen displays. Click Next to continue.



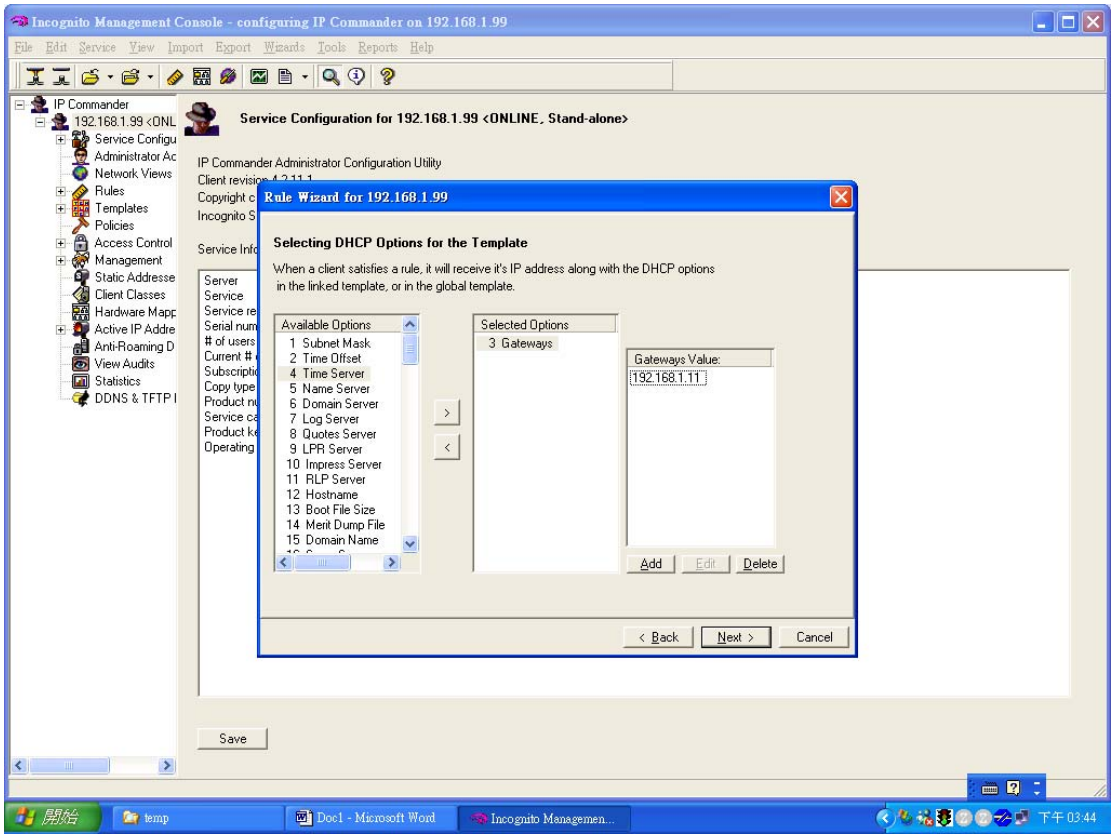
In the next wizard screen, click Next to continue.



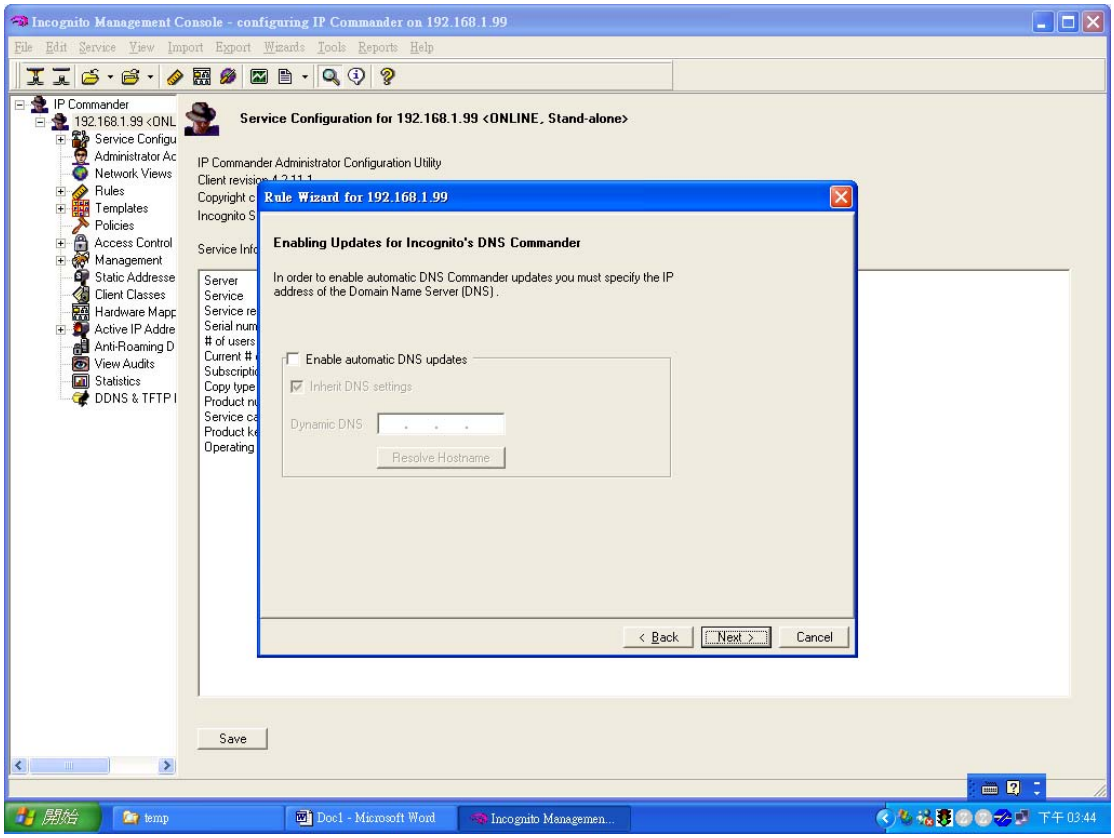
In next screen, you may specify a DHCP template (with the gateway and DNS settings) to use. Here we will create a new template.



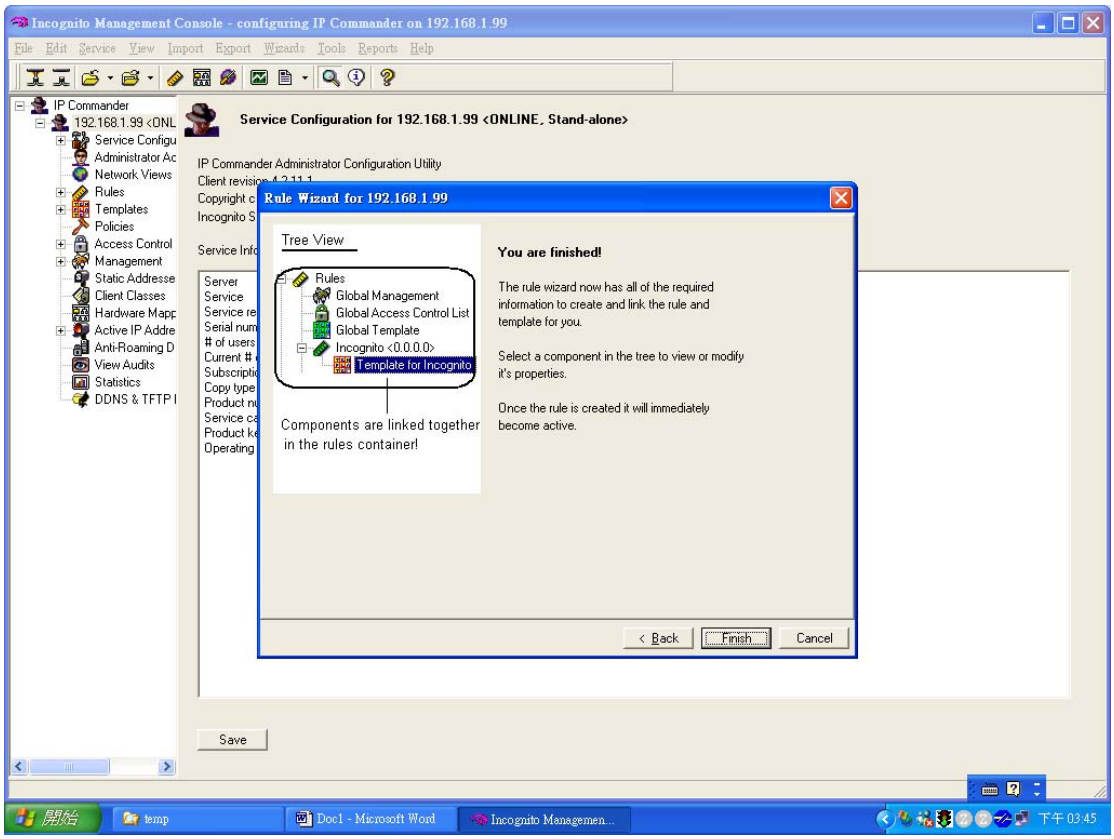
For this template, we enter “192.168.1.1” as the gateway IP address for the DHCP client.



In the next screen, you may choose whether to apply automatic DDNS service on the DHCP server or not.



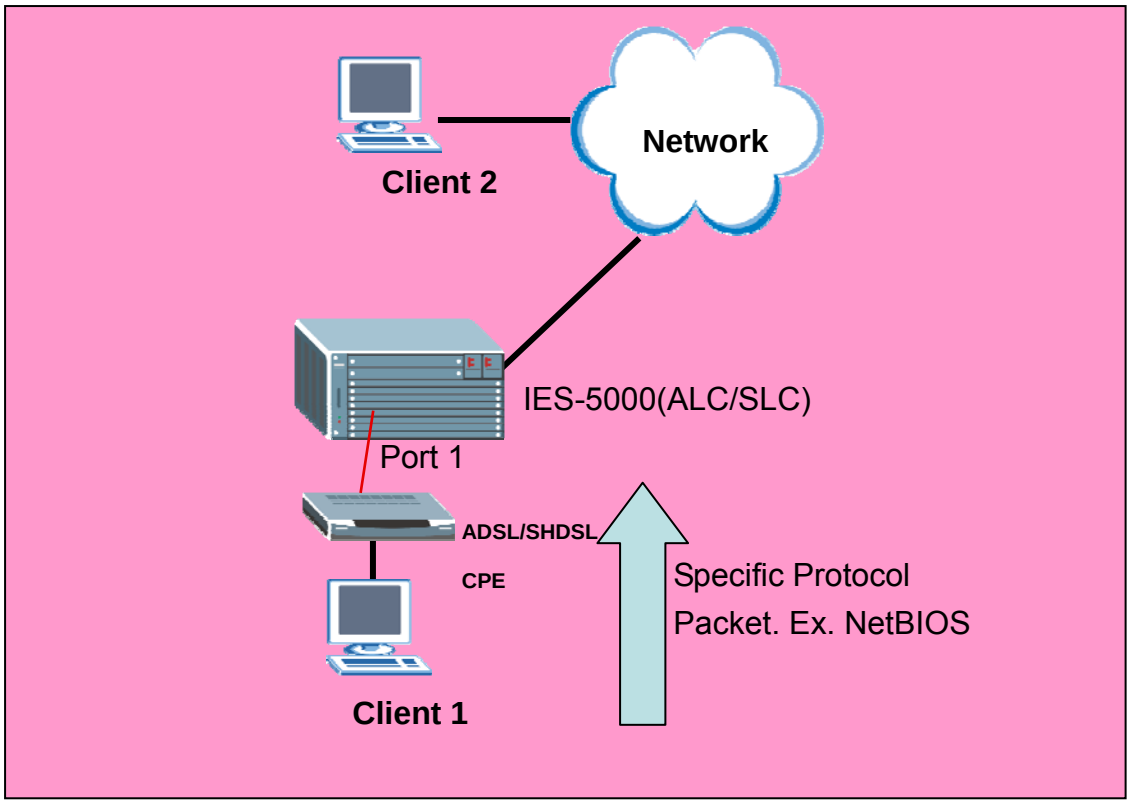
Click Finish to complete the wizard setup.



After the configuration, your computer should obtain an IP address of 192.168.1.201 from the DHCP server once the computer is connected to the network.

Packet Filtering

The packet filtering feature on the IES-5000 allows ISPs to block certain packet types (such as IP, ARP, DHCP, EAPoL, PPPoE, NETBIOS and IGMP).



Setting up Packet Filtering

In this section, we will show you how to configure the IES-5000 to block NETBIOS protocol packets.

1. IES-5000 settings (ALC-1248G/SLC 1248G)

Type the following commands to enable packet filtering on the specific slot-port.

TGE1> lcman port pktfilter set 7-1 netbios

Display packet filtering status on slot 7.

CI command:

```
TGE1> lcman port pktfilter show 7
  port filter
----- -----------------------------------
  7- 1 netbios
  7- 2 accept-all
  7- 3 accept-all
```

7- 4 accept-all
7- 5 accept-all
7- 6 accept-all
7- 7 accept-all
7- 8 accept-all
7- 9 accept-all
7-10 accept-all
7-11 accept-all
7-12 accept-all
7-13 accept-all
7-14 accept-all
7-15 accept-all
7-16 accept-all
7-17 accept-all
7-18 accept-all
7-19 accept-all
7-20 accept-all
7-21 accept-all
7-22 accept-all
7-23 accept-all
7-24 accept-all
7-25 accept-all
7-26 accept-all
7-27 accept-all
7-28 accept-all
7-29 accept-all
7-30 accept-all
7-31 accept-all
7-32 accept-all
7-33 accept-all
7-34 accept-all
7-35 accept-all
7-36 accept-all
7-37 accept-all
7-38 accept-all
7-39 accept-all
7-40 accept-all
7-41 accept-all

```
  7-42 accept-all
  7-43 accept-all
  7-44 accept-all
  7-45 accept-all
  7-46 accept-all
  7-47 accept-all
  7-48 accept-all
TGE1>
```